CJIS - NCJ Policy Manual

A Guide For Fingerprint-Based Access Of Criminal History Record Information
Used For Non-Criminal Justice Purposes

Table Of Contents

SECTION 5: SECURITY AWARENESS TRAINING

SECTION 6: POLICY COMPLIANCE REVIEWS (AUDITS)

SECTION 7: SECURITY & MANAGEMENT CONTROL OUTSOURCING STANDARD

SECTION 8: FINGERPRINT SUBMISSION

SECTION 9: CRIMINAL HISTORY

SECTION 10: STATE AGENCY, BOARD, OR COMMISSION

SECTION 11: VECHS AGENCIES

APPENDICES

BIBLIOGRAPHY

Department of Public Safety
MISSOURI STATE HIGHWAY PATROL
Colonel J. Bret Johnson, Superintendent

An Internationally Accredited Agency

Jeremiah W. (Jay) Nixon
Governor

Lane J. Roberts
Director

October 14, 2015

To: All Agencies with Access to Fingerprint-Based Criminal History Information for Noncriminal Justice Purposes

As the CJIS Division Director, I am pleased to announce the production of a new "CJIS ─ NCJ Policy Manual." This manual is a comprehensive look at "access and use" of state and national criminal history record information based on fingerprint submission for noncriminal justice (civil) purposes.

Created as a supplement to the FBI CJIS Security Policy, it is our goal that this manual will be maintained regularly and provide our users the latest information possible. As a living document, it will reflect changes in policy, technology, and law as they occur; and it will provide each user a dependable, reliable, and easily accessible reference.

Realizing the multiple tasks all of you endure, I would encourage each of you to take the time necessary to become familiar with this manual. It is our hope this document will assist in forming stronger partnerships and promote better compliance with state and federal rules and regulations that govern access. Given the recent and justified scrutiny surrounding this type of information, we hope you will agree these goals are essential to keeping criminal history information available to those who have demonstrated a legitimate need.

As a user of fingerprint-based criminal history, this manual may be incorporated into your own agency policy and procedures by reference. Whether you use the criminal history for employment, licensing, permits, or for some other authorized benefit, this manual will serve to clarify the responsibilities each of us have and will help ensure criminal history information is protected and used according to law.

In closing, the Patrol's CJIS Division is dedicated to providing quality and professional service to our user community, and we look forward to assisting you in any way possible. Included in the manual is a list of contacts available to you should questions or problems arise.

Sincerely,

LARRY W. PLUNKETT, JR., Captain
Criminal Justice Information Services Division

CRIMINAL JUSTICE INFORMATION SERVICES DIVISION
Mailing Address: P.O. Box 9500, Jefferson City, MO 65102-9500
Street Address: 1510 East Elm Street, Jefferson City, MO 65101
Telephone: 573-526-6153 - FAX: 573-751-9382 - V/TDD: 573-751-3313
www.mshp.dps.missouri.gov

SECTION 1: INTRODUCTION

1.1 Mission Statement

The Missouri State Highway Patrol will serve and protect all people by enforcing laws and providing services to ensure a safe and secure environment.

1.2 This Purpose Of This Manual

The purpose of this manual is to provide noncriminal justice agency (NCJA) users with clearly defined guidelines pertaining to use, retention, security, destruction, and dissemination of fingerprint-based criminal history record information (CHRI). It is intended to serve as an easy-to-use source of information, and to provide answers to questions that surface during everyday use of CHRI. In order for all agencies with access to CHRI to operate within the high standards required, all users must have a good understanding of what is expected of them, and comply at all times with established rules and regulations.

The policies and procedures in this manual apply to every individual, contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity, with access to fingerprint-based criminal history record information derived from the systems of the Missouri State Highway Patrol Criminal Justice Information Services Division and U.S. Department of Justice, Federal Bureau of Investigation. This manual serves as a supplement to the FBI CJIS Security Policy and Standard Operating Procedures of the MSHP-CJISD.

1.3 The MSHP-CJISD Is The Central Repository

All collection and dissemination of CHRI is in compliance with Chapter 610 RSMo., Chapter 43 RSMo., and applicable federal laws or regulations. The Missouri State Highway Patrol Criminal Justice Information Services Division (MSHP-CJISD) is responsible for compiling and disseminating complete and accurate criminal history records and for the compiling, maintaining, and dissemination of criminal incident and arrest reports and statistics. CHRI is collected by criminal justice agencies on individuals which consists of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition arising from sentencing, correctional supervision, and release.

Although the primary function of the Central Repository is the administration of criminal justice, the record information retained is available for noncriminal justice purposes. Laws governing the dissemination of open and closed record information are regulated by state statute. (Section 610.120 RSMo., and Title 11 Code of State Regulations (CSR) Division 30, Chapter 4.)

1.4 A Policy Is A Guideline

Guidelines are based on a law or the decisions of a rulemaking authority. Policies help the user understand what may or may not be done with the fingerprint-based CHRI. This manual also dictates sanctions for policy violations.

1.5 A Procedure Is A Method

A procedure is a process or series of steps taken to accomplish a task. Procedures are methods and they are ways of carrying out a policy. The procedures in this manual may dictate actions that must be taken, when and how tasks are achieved, or who takes steps and why they are taken. Procedures also incorporate forms and while some forms are included in Appendix E of this manual, others will be referenced and accessible through the MSHP's website.

SECTION 2: AUTHORITY

2.1 How Policy Is Formulated

The FBI has designated the MSHP-CJISD as the Criminal Justice Information Services (CJIS) Systems Agency (CSA) for the state of Missouri. The superintendent of the MSHP appoints a CJIS Systems Officer (CSO) for the state. The CSO is responsible for ensuring that all agencies with access to CHRI adhere to state and federal laws.

The MSHP has been the Central Repository for fingerprint and criminal arrest information since 1934, when the Bureau of Identification was established within the MSHP. The bureau was not officially designated in state statute until 1986, when the 83rd General Assembly of the state of Missouri passed House Bills 873 and 874. These bills were introduced and overwhelmingly passed based on the premise of the need to protect victims of violent crimes and the need to provide a greater voice to those impacted by crime. On May 12, 1986, legislation was signed and the bills became law in August that same year. Chapter 43 of the Missouri Revised Statutes formally designated the Bureau of Identification as the Central Repository of Missouri. As a result of the passing of these bills, the Missouri State Highway Patrol's Bureau of Identification was designated as the Central Repository for compiling, storing, and disseminating criminal history record information. The bill further required the mandatory reporting of all felony and serious or aggravated misdemeanor criminal arrest information by law enforcement personnel, prosecuting attorneys, courts, Department of Corrections, and the Department of Mental Health. The Central Repository is the sole source communicator of Missouri criminal history records to the FBI. In 1991, the Bureau of Identification was renamed to Criminal Records and Identification Division, and again renamed in 2009, to the Criminal Justice Information Services (CJIS) Division. The CJIS Division functions under the Technical Services Bureau.

The term "non-criminal justice purposes" is defined by the National Crime Prevention and Privacy Compact Council as uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

2.1.1 The *CJIS Advisory Policy Board* (APB) establishes policy concerning the philosophy, concept, and operational principals of the National Crime Information Center (NCIC). It reviews policy, and technical and operational issues in order to make recommendations to the director of the Federal Bureau of Investigation (FBI). The APB is comprised of 33 administrators from local, state, and federal criminal justice agencies throughout the United States and meets at least twice each calendar year.

2.1.2 The *National Crime Prevention and Privacy Compact Council* (Title 42, USC 14611-16), also referred to as "Compact" was signed into law on October 9, 1998, by President Clinton, allowing party states to disseminate their CHRI to other states for noncriminal justice purposes in accordance with the laws of the receiving state. The Compact was necessary to facilitate record sharing as it supersedes any conflicting laws in states where it is adopted and provides a uniform dissemination standard among states. The Compact provides for the establishment of a Council that shall have the authority to

promulgate rules and procedures governing the use of the Interstate Identification Index (III) System for noncriminal justice purposes. The Compact is composed of 15 members appointed by the U.S. attorney general. The membership composition and terms specified under Article VI of the Compact requires nine of the 15 Council members to be state compact officers or state repository administrators. Missouri's Compact officer is Captain Larry W. Plunkett Jr. of the Missouri State Highway Patrol.

2.1.3 The *National Crime Information Center (NCIC)* is maintained by the FBI's Criminal Justice Information Services (CJIS) Division. The purpose of NCIC, according to the FBI, is: "to provide a computerized database for ready access by a criminal justice agency making an inquiry and for prompt disclosure of information in the system from other criminal justice agencies about crimes and criminals. This information assists authorized agencies in criminal justice and related law enforcement objectives, such as apprehending fugitives, locating missing persons, locating and returning stolen property, as well as in the protection of the law enforcement officers encountering the individuals described in the system."

2.1.4 The *Interstate Identification Index (III)* is a "cooperative federal-state program for the interstate exchange of criminal history record information for the purposes of facilitating the interstate exchange of such information among criminal justice agencies." This database was initially created for the use of government agencies involved in the administration of criminal justice functions; however, over time, the use of this information has been authorized for numerous noncriminal justice purposes, such as background screening for employment and licensing. The III system is quite comprehensive in its coverage of nationwide arrest records for serious offenses.

2.1.5 The *Missouri Uniform Law Enforcement System (MULES)* is Missouri's law enforcement computer network. The MULES network was implemented in 1969, within the Information Systems Division (ISD), presently the Information and Communication Technology Division (ICTD), of the MSHP. MULES originated as a computerized information system to serve all criminal justice agencies in Missouri.

2.1.6 The *Automated Fingerprint Identification System (AFIS)* is a computer system that interfaces with criminal history component of MULES and electronically images and stores the characteristics of fingerprint patterns. Fingerprint identification has been a major responsibility of the MSHP since 1934, and the FBI since 1924. The CJIS Division within the FBI is the largest division and is responsible for administering several programs including the Integrated Automated Fingerprint Identification System (IAFIS); the NCIC including the III and other files of interest to law enforcement, such as those relating to wanted persons, civil protection orders, registered sex offenders, and missing persons; and the National Instant Criminal Background Check System (NICS) which processes background checks on prospective purchasers of firearms from federal firearm licensees. (Attorney General Report on Criminal History Background Checks, June 2006.)

2.1.7 CJIS Security Policy — The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of criminal justice information (CJI), whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI data. This policy applies to every individual, including

contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity, with access to, or who operate in support of, criminal justice services and information.

The CJIS Security Policy strengthens the partnership between the FBI and CJIS Systems Agencies (CSA), including in those states with separate authorities, the state identification bureaus. Further, as use of criminal history record information for noncriminal justice purposes continues to expand, the CJIS Security Policy becomes increasingly important in guiding the Compact and state compact officers in the secure exchange of criminal justice records.

The CJIS Security Policy describes the vision and captures the security concepts that set the policies, protections, roles, and responsibilities with minimal impact from changes in technology. The policy empowers CSAs with the insight and ability to tune their security programs according to their needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this Policy. The CJIS Security Policy provides a secure framework of laws, standards, and elements of published and vetted policies for accomplishing the mission across the board spectrum of the criminal justice and noncriminal justice communities.

For viewing and/or download of the CJIS Security Policy, please see Appendix E for the FBI's website link.

2.1.8 Revised Statutes of Missouri (RSMo.) — The MSHP operates and administers the Missouri Uniform Law Enforcement System (MULES) in accordance with the Revised Statutes of Missouri. The following is a summary of pertinent statutes. For full text and other relevant statutes, please refer to Revised Statutes of Missouri. The link is also available in Appendix E.

Section 43.120 RSMo. — The superintendent is responsible for establishing policy, procedures, and regulations to protect the integrity of the MULES system. The superintendent shall be responsible for the administration and enforcement of all MULES policies and regulations.

Section 43.503 RSMo. — For the purpose of maintaining complete and accurate criminal history record information, all police officers of this state, the clerk of each court, the department of corrections, the sheriff of each county, the chief law enforcement official of a city not within a county, and the prosecuting attorney of each county or the circuit attorney of a city not within a county shall submit certain criminal arrest, charge, and disposition information to the Central Repository for filing without undue delay in the form and manner required by Sections 43.500 to 43.543 RSMo.

Section 43.509 RSMo. — Designates the MSHP as the Central Repository for Criminal History Record Information (CHRI).

Sections 577.051 and 302.225 RSMo. — Requires law enforcement agencies to report information on certain traffic convictions to the MSHP, particularly those related to drug or alcohol offenses.

SECTION 3: AGENCY ACCESS

3.1 ORI Assignment

An Originating Agency Identifier (ORI) is a nine-character identifier, assigned by the FBI, and is used to identify authorized agencies and control access to the systems. To qualify for an ORI assignment for noncriminal justice purposes, an agency must be authorized under Public Law 92-544 with an approved state statute or authorized through federal legislation.

3.2 New Agency Application

Requests for access to criminal history must be made to the MSHP-CJISD. A letter of request, along with supporting legislative authority is required. The letter of request should state the purpose for the request and use of criminal history. The letter of request must be sent to the MSHP-CJISD director or the agency may direct questions or correspondence to the regional auditor/trainer for assistance. (Refer to Appendix A for contact information, or Appendix E for sample wording to request an ORI.)

3.3 Public Law 92-544 Requirements

The authority for the FBI to conduct a criminal record check for a noncriminal justice licensing or employment purpose is based upon Public Law 92-544. With this legislation, the FBI is empowered to exchange identification records with officials of state and local governments for purposes of licensing and employment if authorized by a state statute which has been approved by the attorney general of the United States. The attorney general's authority to approve the statute is delegated to the FBI by Title 28, CFR Section 0.85(j). The standards employed by the FBI in approving Public Law 92-544 authorizations have been established by a series of memoranda issues by the Office of Legal Counsel, Department of Justice. The standards are:

1. The authorization must exist as the result of legislative enactment (or its functional equivalent);
2. The authorization must require fingerprinting of the applicant;
3. The authorization must, expressly or by implication, authorize use of FBI records for screening of the applicant;
4. The authorization must not be against public policy;
5. The authorization must not be overly board in its scope; it must identify the specific category of applicants and licensees.

Fingerprint card submissions to the FBI under Public Law 92-544 must be forwarded through the State Identification Bureau (SIB). The state must also designate an authorized governmental agency to be responsible for receiving and screening the results of the record check to determine an applicant's suitability for employment or licensing. (Appendix B Criminal Justice Information Services (CJIS) Information Letter 95-3, Guidelines for implementing the NCPA/VCA Public Laws 103-209, 103-322)

3.4 ORI Structure

Every assigned ORI is unique to that agency. In Missouri, all ORI's will begin with letters "MO" and will be followed by seven characters. A noncriminal justice agency ORI will contain the letter "Z" in the ninth digit. The letter "Z" is used specifically to identify agencies receiving CHRI for noncriminal justice purposes, i.e., employment or licensing or other authorized benefit, according to state statute or federal law. (*Example: MO920320Z is assigned to the Department of Elementary and Secondary Education for use in requesting CHRI based on the authority and purpose in Section 43.543 RSMo.)* An exception to this rule is Missouri Public Housing Authorities (PHAs). ORIs assigned to PHAs will contain the letter "Q" in the ninth digit.

3.5 Proper ORI Usage

ORIs are approved according to state and federal law. Approval and use must be in accordance to the purpose identified in the law. Prior to requesting criminal history for an additional use (a use or purpose not previously approved for the agency), the agency must request permission from the MSHP-CJISD and FBI.

Prior to requesting CHRI for a specific use and purpose, the agency should verify the following:

1. Is the use of CHRI supported by law? If yes, what is the law or statute?
2. If approved in state statute, what purpose(s) are listed as authorized? (This may include employment, licensing, certification, permits, access to children, the elderly, or individuals with disabilities, etc.)
3. Is the agency requesting CHRI for other purposes that are not identified in their approved statute?

***Example 1 — Question**: A city government has an ORI approved through a local ordinance and Section 43.535 RSMo. for liquor licensing and city employment. The city wants to do background checks for taxi cab drivers. Are they authorized? Answer: No.*

Recommendation: Prior to requesting CHRI for an additional use, the city is required to amend the local ordinance or pass a new ordinance and submit a letter of request to the MSHP-CJISD. Prior to using the existing ORI for a subsequent use, approval must be given by the FBI.

***Example 2 — Question**: A state agency has an ORI, approved through a state statute for state employment. They want to do background checks on volunteers. Is this authorized?*

Recommendation: The answer depends on the statute through which the agency is currently approved. If the word "volunteer" is included in the statute that they are currently using, they would be authorized. However, if the word "volunteer" is not included, they would not be authorized. Example: Agency is approved under Section 43.543 RSMo. for employment. Because "volunteer" is not included in this statute, the agency would not be authorized. However, by requesting that Section 43.540 RSMo. be

added to the agency's authorization, the agency would be authorized. The FBI would need to approve the additional statute prior to any submission.

Listed below is a sampling of agencies approved under Public Law 92-544 and Missouri Revised Statutes. The CHRI requested is used primarily for employment, licensing, certifications, permits.

- Missouri Department of Elementary and Secondary Education
- Missouri Division of Professional Registration
- Missouri Department of Mental Health
- Missouri Department of Social Services
- Missouri Lottery Commission
- City and County Governments
- Missouri Veterans Commission
- Missouri Veterans Homes
- Missouri Department of Revenue
- Office of State Courts
- State of Missouri, Office of Administration
- Missouri Department of Transportation
- Missouri Judicial Courts
- Law Enforcement Agencies
- Metropolitan Taxicab Commission
- Missouri Department of Insurance

Listed below is a sampling of agencies approved through federal legislative Acts. The CHRI requested is used for various purposes.

- VECHS agencies, authorized through the National Child Protection Act, as amended by Volunteers for Children Act (NCPA/VCA) and the Adam Walsh Act. VECHs is for those entities providing care to children, the elderly, or individuals with disabilities (i.e. child care facilities, churches, private elementary and secondary schools, private colleges, adoption agencies, healthcare professionals, private bus companies, private nonemergency medical transportation agencies, learning/tutoring facilities).
- Public Housing Authorities (PHAs) for housing applicants, evictions, lease enforcement, based on Public Law 104-120, Title 42, and the Housing Opportunity Program Extension Act of 1996.
- Private security guard agency's based on the Private Security Officer Employment Authorization Act of 2004, Public Law 108-458, Title 28, CFR, Part 105, Subpart C.

Access to CHRI requires an assigned Missouri ORI with state or federal law and a current user agreement with the MSHP-CJISD. All approved entities are audited on a triennial basis.

3.6 User Agreement

Per the CJIS Security Policy, each agency with access to criminal justice information (CJI) must have a current user agreement signed by the agency representative and the MSHP-CJISD. The user agreement must be updated in the event of an entity representative change. CJI is criminal history record information.

The purpose of the user agreement is to provide CHRI to authorized employers, licensing agencies, and other agencies requesting fingerprint-based CHRI. Fingerprint-based CHRI must be explicitly mandated or allowed by law. National (FBI) CHRI must be authorized by federal law or a state statute approved by the U.S. attorney general, pursuant to Public Law 92-544. The applying agency is known as "authorized recipient" (AR).

The user agreement states that the MSHP-CJISD will:

1. Provide CHRI in response to fingerprint-based background checks, either to the AR or to the appropriate agency that reviews CHRI results for the AR pursuant to an approved Outsourcing Standard. (See Section 7, Outsourcing Standard.)
2. Provide assistance to the AR in interpreting CHRI.
3. Work to ensure the completeness and accuracy of the CHRI.
4. Conduct audits to assure compliance with this user agreement, state and federal laws, and pursuant to the FBI CJIS Security Policy.
5. Cease providing information to the AR if the user agreement is violated or if the AR is suspected of violating the agreement.

The AR agrees to the following:

1. Abide by the terms and conditions identified in the agreement.
2. Comply with state and federal laws, rules, procedures, and policies, including those adopted by the state, the MSHP-CJISD, and the National Crime Prevention and Privacy Compact (42 U.S.C. 14611-16) regarding the receipt, use, and dissemination of CHRI.
3. Use CHRI only for the purpose for which it was requested.
4. Provide for the security of any CHRI received. This includes, but is not limited to:
    - Designate a local agency security officer (LASO) who is responsible for ensuring compliance with security procedures and the user agreement.
    - Ensure that all personnel with access to CHRI are aware of the rules and responsibilities with regard to CHRI, pursuant to the most current version of the CJIS Security Policy.
    - Restrict access to physical or electronic copies of CHRI to authorized personnel. Physical copies shall be maintained in a controlled, secure environment such as a locked cabinet in a room not accessible to all staff and visitors. Electronic copies shall be protected with at least 128-bit encryption or individually password protected. The relevant federal encryption standard is FIPS 140-2.
    - Restrict dissemination of CHRI unless explicitly allowed by law and log all authorized dissemination. Logs shall include at a minimum: the date, the name of sending agency,

name of receiving agency or applicant, record shared, means of dissemination, and name of person who disseminated.
- Track and report information security incidents such as the theft/loss of physical records or the penetration of electronic systems.
- Dispose of records securely. Physical media should be cross-shredded at a minimum, and electronic records should be deleted and repeatedly over-written with random 0s and 1s.

5. Understand that this data is based on CHRI received at the state repository and through the systems of the FBI. If a person could be adversely affected by this data, the person must be given the opportunity to challenge and correct a record. Challenge and/or appeal procedures are referenced in Section 43.532 RSMo. and Title 28, Code of Federal Regulations (CFR) 16.30-34.
6. Retain audit records for at least three years or until AR has received a favorable compliance rating from a MSHP-CJISD Policy Compliance Review. Once the minimum retention time period has passed, the AR shall continue to retain audit records until they are no longer needed for administrative, legal, audit, or other operational purposes such as the Freedom of Information Act requests or legal actions.
7. Allow the MSHP-CJISD to conduct audits to assure compliance with the agreement.
8. Pay all fees for CHRI provided by the MSHP-CJISD and FBI in accordance with Section 43.530 RSMo. and Title 28 CFR 20.31(e)(3).

The AR must understand that the CHRI has the following limitations and contains three parts: (a) the arresting agency's name and crime class under which the person was arrested. The arrest data submitted includes the mandatory field of name, race, sex, and date of birth. All arrests are accompanied by fingerprints; (b) the charge(s) issued by the prosecutor; and (c) the name of the court that tried the case and the ultimate disposition of the case.

CHRI and custody information is compiled from information submitted to the MSHP-CJISD from law enforcement agencies, prosecutors, courts, Department of Mental Health and Department of Corrections (referred to as contributing agencies.) Although the MSHP-CJISD makes reasonable efforts to ensure all information is submitted as required by law, it is not responsible for omissions from contributing agencies.

Before releasing information on individuals or taking adverse action against an individual listed on the CHRI, the person in question must be afforded the opportunity to dispute and correct the record.

CHRI is constantly being updated as new arrests and other information are entered into the system by contributing agencies. The record released is only valid as of the date the criminal history record check was performed. Certain statutes allow for the suppression or deletion of records and this information is not provided. (Expungements — Sections 610.122, 610.123, 610.140 and 577.054, 575.120 RSMo.)

The MSHP-CJISD retains records for the state of Missouri only. Most fingerprinting reasons include a check through the FBI, which the MSHP-CJISD will request on the AR's behalf as a normal part of the criminal history record check, when allowed by law.

The user agreement commences on the date the last signature is obtained on the document and continues until terminated by either party. The user agreement may be terminated sooner by one or both parties upon 30-days' written notice or immediately upon violation of the terms of the user agreement.

3.6.1 User Agreement for Missouri VECHS Program Entities — The same user agreement requirements stated above are applicable to VECHS program entities with the exception that VECHS entities must use a Waiver Agreement and Statement (SHP-981) prior to receiving CHRI on their applicants. The user agreement on file between the MSHP-CJISD and VECHS approved entities includes additional wording for the Waiver Agreement and Statement requirement.

The waiver is required since the authority to receive CHRI is based on federal law and not approved in state statute or as stipulated in Public Law 92-544. Although the approval is through federal legislative Acts, the use of a waiver is a federal requirement and incorporated into VECHS program documents. It is important to note that prior to a VECHS entity requiring an applicant to submit fingerprints, the entity must provide the waiver to the applicant for review and signature. The waiver gives the entity permission to request and receive CHRI from the systems of the MSHP and FBI. The signed waiver must be retained by the entity for audit purposes. Failure to obtain the waiver may result in suspension of services. (Refer to Section 11 for more information about VECHS.)

3.7 Applicant Privacy Rights

During the May 2012 National Crime Prevention and Privacy Compact Council meeting, the Compact Council vetted the "Guiding Principles" for advising agencies receiving federally maintained criminal history record information of their obligation to notify applicants of their rights in accordance with Title 28 CFR 50.12 regarding the exchange of FBI identification records. Records obtained under this authority may be used solely for the purpose requested and cannot be disseminated outside the receiving departments, related agencies, or other authorized entities. Officials at the governmental institutions and other entities authorized to submit fingerprints and receive FBI identification records under this authority must notify the individuals fingerprinted that the fingerprints will be used to check the criminal history records of the FBI.

The officials making the determination of suitability for licensing or employment shall provide the applicant the opportunity to complete or challenge the accuracy of the information contained in the FBI identification record.

These officials also must advise the applicant that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28 CFR 16.30-34. Officials making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.

This policy is intended to ensure that all relevant criminal record information is made available to provide for the public safety and, further, to protect the interests of the prospective employee or

licensee who may be affected by the information, or lack of information in an identification record. (Order No. 2258-99, 64 FR 52229, September 29, 1999.)

3.7.1 Agency Requirements for Applicant Privacy Rights — Each agency will be assessed on the requirements stated in the *Agency Requirements for Noncriminal Justice Applicants*, pursuant to federal legislation.

Authorized governmental and non-governmental agencies and officials that conduct a national fingerprint-based criminal history record check on an applicant for a noncriminal justice purpose (such as a job or license, immigration or naturalization matter, security clearance, or adoption) are obligated to ensure the applicant is provided certain notice and other information and that the results of the check are handled in a manner that protects the applicant's privacy.

Officials must provide to the applicant written notice that his/her fingerprints will be used to check the criminal history records of the FBI.

Officials using the FBI criminal history record (if one exists) to make a determination of the applicant's suitability for the job, license, or other benefit must provide the applicant the opportunity to complete or challenge the accuracy of the information in the record.

Officials must advise the applicant that procedures for obtaining a change, correction, or updating of an FBI criminal history record are set forth at Title 28 CFR Section 16.34.

Officials should not deny the job, license, or other benefit based on information in the criminal history record until the applicant has been afforded a reasonable time to correct or complete the record or has declined to do so. (Reasonable time is determined by agency.)

Officials must use the criminal history record solely for the purpose requested and cannot disseminate the record outside the receiving department, related agency, or other authorized entity. (28 CFR 50.12)

The FBI has no objection to officials providing a copy of the applicant's FBI criminal history record to the applicant for review and possible challenge when the record was obtained based on positive fingerprint identification. If agency policy permits, this courtesy will save the applicant the time and additional FBI fee to obtain his/her record directly from the FBI by following the procedures found at 28 CFR 16.30 through 16.34. It will also allow the officials to make a more timely determination of the applicant's suitability.

Each agency should establish and document the process/procedure it utilizes for how/when it gives the applicant notice, what constitutes "a reasonable time" for the applicant to correct or complete the record, and any appeal process that is afforded the applicant. Such documentation will assist state (MSHP) and/or FBI auditors during periodic compliance reviews on use of criminal history records for noncriminal justice purposes.

The documents *Agency Privacy Rights for Noncriminal Justice Applicants* and *Noncriminal Justice Applicant Privacy Rights* are available on the FBI's website and the MSHP's website. The links are also in Appendix E.

SECTION 4: SECURITY AND ACCESS

4.1 Guidelines For Access & Use

Information obtained from the III is considered criminal history record information (CHRI). Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, and Code of Federal Regulations (CFR). The III shall be accessed only for an authorized purpose. Furthermore, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed.

4.2 Restrictions

CHRI is restricted to only those entities that have been determined to be qualified entities. Qualified entities are those entities authorized in state legislation (i.e. Missouri approved state statute) or federal legislation (i.e. the Adam Walsh Act, the National Child Protection Act). Authorized entities in Missouri will have an ORI which was approved by the FBI based on legislative authority. Unlawful dissemination is a class A misdemeanor offense. (Sections 576.050, 43.532, 43.540 RSMo. and Title 28 CFR 50.12)

4.3 Retention/Storage Of CHRI/CJI

When CHRI is stored, agencies shall establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files.

Retention of criminal history record information is not required. It is also not needed for compliance reviews/audit purposes.

If your agency policy is to retain the CHRI/CJI, you must ensure the following:

1. The record information must be kept in a secure records environment and free from public or unauthorized access.
2. The area that contains the record information must be secured by lock and with limited access.
3. When retained in electronic media, the data must be protected with a password and/or encryption. (See Section 4.3.1 of this manual.)

If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CHRI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CHRI access or storage. The agency shall, at a minimum:

1. Limit access to the controlled area during CHRI processing times to only those personnel authorized by the agency to access or view CHRI.

2. Lock the area, room, or storage container when unattended.
3. Position information system devices and documents in such a way as to prevent unauthorized individuals from access and view.

4.3.1 Electronic Retention — Media protection policy and procedures shall be documented and implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting, and storing media.

The agency shall securely store electronic media within secure locations or controlled areas. The agency shall restrict access to electronic media to authorized individuals. If personnel restrictions are not feasible, then the data shall be encrypted. Encryption shall be a minimum of 128 bit.

Electronic media means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

Controls shall be in place to protect electronic media while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute other controls to ensure security.

4.3.2 Retention/Storage Off-Site — Procedures for handling and storage of information shall be established to protect the information from unauthorized disclosure, alteration, or misuse. The procedures shall apply to the handling, processing, storing, and communication of CHRI. These procedures apply to the exchange of CHRI no matter the form of exchange.

The agency shall protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

Prior to storage of CHRI off-site and under the control of a third party, the agency is required to obtain an Outsourcing Management and Control Agreement prior to allowing a third party access to or storage responsibilities. Outsourcing must be approved by the MSHP-CJISD prior to any off-site storage. (See Section 7 of this manual for more information about Outsourcing.)

4.4 Destruction Of CHRI

It is recommended that on-site destruction be completed at the agency by authorized agency personnel. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

If your agency contracts with a private destruction company, the destruction must take place under the direct supervision of authorized agency personnel. If any agency allows destruction of criminal history

records to occur off-site, a Management and Control Outsourcing Agreement is required prior to access by a private vendor. (See Section 7 of this manual for Outsourcing.)

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media should be cross-shredded at a minimum.

For electronic media, the agency shall sanitize, that is, overwrite with random 0s and 1s at least three times or degauss the electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

4.5 Security of CHRI — Personnel Access to CHRI

Pursuant to CJIS Security Policy, Appendix J, Noncriminal Justice Agency Supplemental Guidance, agencies located within states having passed legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to CHRI for the purposes of licensing or employment shall follow the guidance in the CJIS Security Policy which requires the submission of fingerprints. However, agencies located within states without this authorization or requirement are exempt from the fingerprint-based background check requirement until such time as appropriate legislation has been written into law.

Although fingerprint-based background checks are not required for noncriminal justice agencies and personnel at this time, the MSHP-CJISD recommends, as a best business practice, that individuals with access to CHRI have a fingerprint-based background check completed through the MSHP-CJISD and FBI.

4.6 Dissemination Of CHRI

Primary dissemination of CHRI is when the MSHP-CJISD disseminates to an authorized recipient. The MSHP-CJISD will not disseminate CHRI to the subject of record when the fingerprint submission and resultant CHRI is requested by an authorized recipient, i.e., the holder of the ORI. Secondary dissemination of CHRI must be obtained through the authorized recipient and is at the authorized recipient's discretion, i.e. when agency policy allows.

Dissemination to another agency is authorized if the other agency is an authorized recipient (AR) of such information. Authorization must be pursuant to state and/or federal law and the AR must have a current user agreement with the MSHP-CJISD.

Dissemination of CHRI includes all forms such as, but not limited to, verbal, hard copy, electronic, email, and facsimile. It is recommended that agencies have a specific policy in place for dissemination to ensure that any and all dissemination is in accordance with state and federal laws. Dissemination of CHRI may be through U.S. Mail or in person with an authorized recipient or to the applicant/subject of

record. Dissemination via email and facsimile is not authorized unless the agency has appropriate controls in place for secure transmission. (Refer to Section 5, Security Awareness Training, Email & Email Attachments.)

Criminal history records may be used solely for the purpose requested and cannot be disseminated outside the receiving departments, related agencies, or other authorized entities. (Title 28, CFR 50.12)

Any information received by an authorized state agency or a qualified entity ... shall be used solely for internal purposes in determining the suitability of a provider. The dissemination of criminal history information from the FBI beyond the authorized state agency or related governmental entity is prohibited. All criminal record check information shall be confidential and any person who discloses the information beyond the scope allowed is guilty of a class A misdemeanor. (Section 43.540 RSMo.)

4.6.1 Dissemination Authorized

The FBI and MSHP have no objections to officials providing a copy of the applicant's FBI and state CHRI to the applicant for review and possible challenge when the record was obtained based on positive fingerprint identification. If agency policy permits, this courtesy will save the applicant time and additional state and FBI fees to obtain the record(s). (Title 5, United States Code Section 552a, Privacy Act of 1974)

When dissemination is to the subject of record in person, the person must show photo ID and sign a secondary dissemination log. When dissemination is through U.S. Mail, the log must indicate to whom and where the CHRI was mailed.

Dissemination is authorized to other entities subject to verification that the requesting entity is an authorized recipient. Authorization must be through state or federal law and must be through the same authority (Public Law 92-544 or federal laws). **The requesting entity must have a current user agreement on file with the MSHP-CJISD. The requesting entity must be a Missouri agency with a physical operating address in Missouri and must have the same legislative authority with same scope and purpose for use of the record information**.

4.6.2 Public Hearing/Access

CHRI must not be disseminated to the general public. This includes maintaining CHRI in formats that are accessible by the public or within records that are subject to release through public record requests. However, CHRI may be disclosed as part of the adjudication process during a hearing that is open to the public if the agency demonstrates: 1) the hearing is based on a formally established requirement; 2) the applicant is aware prior to the hearing that CHRI may be disclosed; 3) the applicant is not prohibited from being present at the hearing; and 4) CHRI is not disclosed during the hearing if the applicant withdraws from the application process. For example, a board or commission may be authorized to access CHRI, and as part of regularly scheduled meetings, applicant appeals are discussed as standard agenda items. Even when the specific conditions are met to allow disclosure during a public hearing, the

most preferable method for introducing CHRI is to enter into a closed session which limits participation by the public at large. States and local agencies should be able to reasonably demonstrate how the prerequisite criteria are being met for audit purposes.

4.6.3 Jurisdictional Control

Agencies outside of a state's jurisdiction cannot be designated as related agencies, even when a congruent related need appears to exist for the use of CHRI. The dissemination restriction primarily centers on each state's individual authority and obligation to administer access to CHRI. Each state has the authority to determine whether or not to conduct particular types of noncriminal justice background checks, and each state is responsible for establishing the mechanisms and procedures for those checks within its jurisdiction. In addition, each state possess limited authority to meet obligations for maintaining appropriate controls, such as user agreements and audits, outside of its jurisdiction, especially with respect to another state's governmental agencies. In conjunction with the more obvious jurisdictional concerns associated with one state's governmental agency leveraging another state's statutes under Public Law 92-544, similar jurisdictional concerns also exist with the use of other statutory authorities such as the Adam Walsh Act or the NCPA/VCA.

Dissemination is authorized to:

- The subject of the record, and
- Other Authorized Recipients as allowed by law

Some examples of authorized entities under same legislative authority include:

- VECHS agency to another VECHS agency;
- Housing authority to another housing authority;
- State agency to state agency under same legislative authority. (Note: State statutes are approved pursuant to Public Law 92-544 and, therefore, any state agency or other agency with authority through state statutes is authorized to disseminate with each other, however, **the use of CHRI must be for the same scope and purpose**.)

4.6.4 Dissemination Unauthorized

Examples of unauthorized dissemination include:

1. One state governmental agency sharing CHRI with another state's governmental agency for adoption purposes when the child and prospective parents reside in different states, even if both states have approved Public Law 92-544 state statutes.
2. Criminal history sharing initiatives involving participation in national compacts, associations, or databases such as those for child placement or employment/licensing in the health care industry.

This dissemination restriction is not intended to limit a state from making CHRI available in very limited situations to certain nongovernmental entities outside of the state's geographical boundaries when such dissemination is specifically authorized and formal jurisdictional authority is established to maintain adequate controls. It is very important to recognize that in order for dissemination to occur beyond a state's geographical boundaries, there must first be an approved statutory authority which allows

nongovernmental entities access to CHRI within the state's geographical boundaries. There must also be a recognized authority and obligation to formally establish security controls over the nongovernmental entities. For example, it is acceptable for a state to leverage an out-of-state private contractor for record archiving and destruction, since access to CHRI by private contractors is authorized pursuant to Title 28, C.F.R., Part 906, and jurisdictional authority for controls such as audits would be formally established through implementation of the *Security and Management Control Outsourcing Standard for Non-Channelers*. (Ref: NCJ Online Policy Resource document dated 3/18/2015.)

Additional examples of unauthorized dissemination include:

1. Sharing CHRI across state lines or outside of Missouri is strictly prohibited.
2. Do not disseminate to unauthorized agencies or individuals, which include family members or friends of the subject of record. Unauthorized agencies include, but are not limited to, those agencies that do not have legislative authority, do not have an ORI, and do not have a current user agreement with the MSHP-CJISD.
3. Do not store or retain CHRI on a server that is unprotected and is accessible from out of state or by an unauthorized entity.
4. Do not disseminate CHRI to a relative, spouse, or friend of the subject of record.
5. Do not disseminate CHRI to an independent or third-party auditor, such as a corporate auditor, national program or grant program auditor, etc. Authorized auditors are employees of the MSHP-CJISD and FBI.
6. Do not disseminate CHRI to an agency approved under different legislative authority (Public Law 92-544 agencies and those approved under federal legislation.) Examples: VECHS agencies approved under NCPA/VCA, Adam Walsh Act, or Serve America Act are only allowed to disseminate to other VECHS agencies for the same scope and purpose and only after confirming that the other agency is an active VECHS agency with a valid user agreement. Public Housing Authorities (PHAs) approved under Public Law 104-120 are only allowed to disseminate to other PHAs and only after confirming that the housing authority has an approved ORI and a valid user agreement. State agencies or other agencies that are named in Missouri state statute or approved through Missouri state statute are allowed to disseminate with each other if for the same scope and purpose and only after confirming that the requesting agency has an ORI and has a valid user agreement. The FBI has indicated that cross-sharing of CHRI to agencies approved through different legislative authority is not authorized (FBI CJIS Audit August 2012).
7. Do not disseminate CHRI by electronic medium such as facsimile (fax) or email unless proper safeguards are in place to protect the transmission.

As a "best business practice," dissemination should be limited to the subject of record or applicant. Therefore, any further dissemination would be the applicant's decision. When in doubt regarding dissemination, do not disseminate and contact your regional auditor/trainer for assistance.

4.7 Dissemination Log Standards

Secondary dissemination occurs when a criminal history is passed from one agency or ORI to another agency or ORI. For law enforcement agencies, as a minimum standard, NCIC requires that secondary dissemination be logged. The log must contain the name of the subject of record, the signature of the

person releasing the criminal history, and the name of the person receiving the criminal history and dissemination logs may be kept in different formats, such as electronic or hard copy.

The following is the established minimum standard for a secondary dissemination log for noncriminal justice purposes. The log must contain:

1. The name of the subject of record/applicant;
2. The name of the person and/or agency requesting the record;
3. The purpose for the request;
4. The name of the person releasing the record;
5. The date released; and
6. Signature of the person receiving the record when receiving in person. (When disseminated through U.S. Mail, show address.)

When disseminating, it is recommended that the original criminal history record response remain with the original authorized recipient and that a copy be provided to the applicant or authorized requesting agency. The copy should be marked as "copy" and the secondary dissemination log must be retained by the disseminating agency for at least three years or until the agency has received a current policy compliance review (audit).

The tracking of dissemination can be in many forms:
1. The agency may develop and use a standardized form. (See sample in Appendix E.)
2. The agency may log by way of written correspondence, such a letter to the agency or applicant.
3. The agency may use a copy of electronic correspondence that was sent to an agency or applicant. (Reminder: Prior to any electronic dissemination, the agency must have proper safeguards in place.)

All logs or tracking mechanisms for secondary dissemination must adhere to the minimum standards.

4.8 Misuse Of CHRI

Section 43.540 RSMo. Any information received by an authorized state agency or a qualified entity pursuant to the provisions of this section shall be used solely for internal purposes in determining the suitability of a provider. The dissemination of criminal history information from the Federal Bureau of Investigation beyond the authorized state agency or related governmental entity is prohibited. All criminal record check information shall be confidential and any person who discloses the information beyond the scope allowed is guilty of a class A misdemeanor.

Section 43.532 RSMo. Criminal history and identification records obtained from the Central Repository shall be used solely for the purpose for which they were obtained. The subject of the record shall be afforded the opportunity to challenge the correctness, accuracy, or completeness of a criminal history record.

The Central Records Repository shall have authority to engage in the practice of collecting, assembling, or disseminating criminal history record information for the purpose of retaining manually or

electronically stored criminal history information. Any person obtaining criminal history record information from the central repository under false pretense, or who advertises or engages in the practice of collecting, assembling, and disseminating as a business enterprise, other than for the purpose of furnishing criminal history information to the authorized requester for its intended purpose, is guilty of a class A misdemeanor.

Section 576.050 RSMo. A person commits the crime of misuse of official information if he or she knowingly or recklessly obtains or discloses information from the Missouri Uniform Law Enforcement System (MULES) or the National Crime Information Center System (NCIC), or any other criminal justice information sharing system that contains individually identifiable information for private or personal use, or for a purpose other than in connection with their official duties and performance of their job. Misuse of official information is a class A misdemeanor.

SECTION 5: SECURITY AWARENESS TRAINING

5.1 Security Awareness Training Overview

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to criminal justice information (CJI). Access to CJI includes direct access or access to CJI through fingerprint submission.

CJI is any information collected by the FBI, MSHP, or other criminal justice entities. It is available to anyone who is authorized to use CJIS systems. CJI is not limited to criminal history or information available through MULES, and includes personally identifiable information (PII) and other derived information.

The responsibility of each agency and person with access to CJI is to know that the information contained within the CJIS information systems is sensitive information. Improper access, use, and dissemination of CJIS data is serious and may result in the imposition of administrative sanctions including termination of services, as well as state and/or federal criminal penalties. Each person with access to CJI has a responsibility to protect the information and report security incidents.

5.1.1 What Happens If A Person Misuses CJI? A person commits the crime of misuse of official information if he or she knowingly obtains or recklessly discloses information from the MULES or the NCIC, or any other criminal justice information sharing system that contains individually identifiable information for private or personal use, or for a purpose other than in connection with their official duties and performance of their job. Misuse of official information is a class A misdemeanor.

Each person with access of CJI should only use the information to perform their job duties. Disseminating or sharing CJI with anyone that is not authorized to have access to the information is strictly prohibited. If releasing the CJI to another authorized agency, a secondary dissemination log must be kept**. All CJI must be protected from creation through destruction.** ***When disseminating, be aware of where the information could go if rel*****eased.**

If your agency has a security incident, each person within your agency should know to report incidents to the local agency security officer (LASO) of your agency. The LASO is responsible for reporting the incident to the appropriate people at the MSHP-CJISD.

The LASO is responsible for:

- Maintaining the list of users who have access to CJI.
- Identifying how equipment is connected to MSHP (if applicable).

- Ensuring proper personnel screening procedures are being followed, such as fingerprint background check of personnel having access to CJI. (Recommended for NCJA agencies, but not required at this time.)
- Notify MSHP ISO of any security incidents. (Security Incident Report form is located in Appendix E.)

Each agency is responsible for having a Security Incident Response Plan. The plan should be part of your agency policy and procedures. If you are suspicious of something, report it through your agency's procedures. It is better to have multiple false alarms than to miss one incident. The plan extends to a threat against "any CJI," not just computer related — it also includes physical media.

An incident is the act of violating an explicit or implied security policy. Some examples include, but are not limited to:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data;
- Unwanted disruption or denial of service;
- The unauthorized use of a system for the processing or storage of data;
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

5.1.2 Media Protection & Disposal — The protection must include both physical and electronic media and includes Flash Drives, Hard Drives, CD, DVD's, documents, pictures, etc. All media must be stored in secure areas and should be granted to authorized personnel only. Make sure that printed information is printed to the correct printer. All CJI data located, transmitted, or transported outside a secure location must be encrypted, according to FBI standards, or carried in a locked container and protected in transit. When in transit, it should be carried in locked container or folders where it is not visible to the public. When destruction is necessary, electronic media must be physically destroyed or overwritten three times and shredded or incinerated.

5.1.3 Physical Security Of CJI — In order to handle or process CJI, staff and equipment must be in a secure location. The location could be a building, room, or area, and the area should be marked. A list of authorized users must be maintained. The area must have controls such as locks. Monitors and printers must be secure in order to prevent unauthorized viewing of CJI.

5.1.4 Threats — Be aware of the different types of threats, which include (a) natural threats, (b) unintentional threats, and (c) intentional threats. A threat is an unintentional or deliberate event or circumstance which could have an adverse impact on an information system. Threats can come for internal or external sources and vulnerabilities lead to threats. Further explanation of threats is as follows:

- Natural threats can endanger any facility or piece of equipment. You may not be able to prevent a natural disaster, but damage can be minimized with proper planning. Natural threats include fire, flood, lightning, and power failures.
- Unintentional threats are actions that occur due to lack of knowledge or through carelessness. These threats can be prevented through awareness and training. Unintentional threats include

physical damage to equipment, deleting information, and permitting unauthorized users to access information.

- Intentional threats are those threats that are deliberately designed to harm or manipulate an information system, its software, and/or data. Security software such as an antivirus program is designed to protect against intentional threats. Intentional threats include social engineering, phishing, sabotage, eavesdropping, unauthorized data access, intrusions, denial of service, theft, etc.

5.1.5 Password Policy For CJI — Your agency's password policy should be a minimum length of eight characters. It cannot be a dictionary word or proper name and cannot be the user ID. The password should be set to expire every 90 days and cannot be identical to the previous 10 passwords. It cannot be displayed when entered. Each person with access should be advised to not share their password with anyone, including the agency IT staff. Passwords should not be written down and do not use increment numbers in the passwords. Do not make it easy to type or use keyboard patterns. Some hints for good passwords are to use phrases or run words together. Substitute special characters for common letters ($0somethingeasy2remember.)

5.1.6 Email & Email Attachments — Email is NOT a secure method of communication. As a general rule, do not send anything in an email that you do not want others to see. Do not send CJI in an email unless you know that proper technical controls are in place to protect it, such as encryption and access control. All email should be scanned for known viruses and spam, but it is still an easy avenue for malicious code.

5.1.7 Internet Policy — Internet should be monitored and controlled. All devices that connect to the Internet should be protected by a firewall.

5.1.8 Social Engineering is the attempt to gather information by deception. Scams and phishing attempts are the major categories of social engineering. Social engineering could come from any source such as email, telephone, or face-to-face communication. It will not be obvious that the person is trying to gather information and could be masked as a marketing call. If you are suspicious, do not answer and report the incident. Never respond to an email asking for personal or confidential information, especially if it comes from someone you do not know.

5.1.9 Laptop, Handheld, & Personal Devices — There are many personal and work-related devices available. Each user should know the agency policy of using these devices. Personal devices are NOT allowed to access CJI systems. Devices need to be secure and managed by the agency IT staff and need to be password protected and encrypted. If lost or stolen, report it as an incident. Laptops must be encrypted. Lock computer before stepping away from the work area. CJI should not be stored, accessed, or viewed from personal computing equipment, and should not be accessed from a library, school, or hotel computers.

5.1.10 Access Requests — The access request process should be a documented process. The main focus is separation of duties and least privileged access. A person who authorizes access should not have the ability to implement the request. The level of access should be enough to perform the job duties. Do

not give higher authority to a person unless needed. If your user ID is compromised and you have the least level of access, less information is at risk.

5.2 Security Awareness Training Online Resource

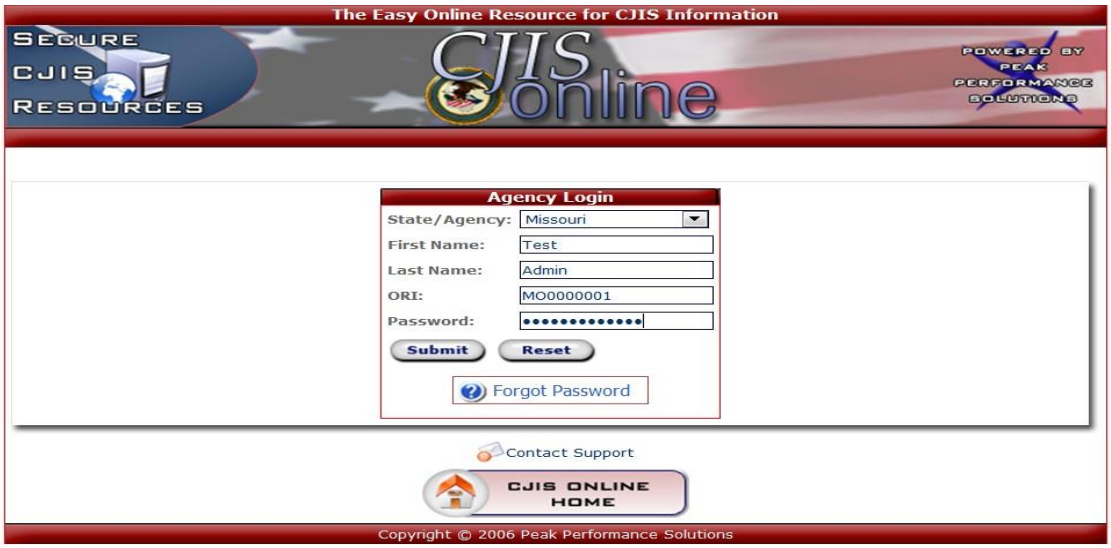
Go to: www.cjisonline.com

1. You need a User ID and password — **both are assigned by the MSHP-CJISD**. Upon signing into your account the first time, you will have the option of changing your password.

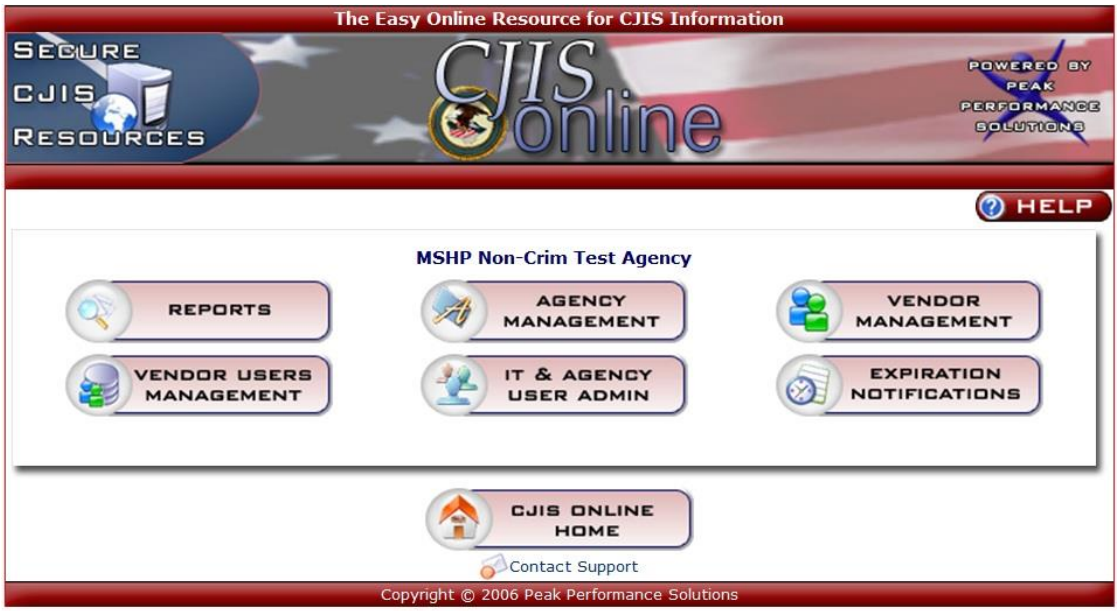
2. Select "Local Agency Admin."

NOTE: Do not select "CJIS Security Training." As a new user, you are required to login first, through "Local Agency Admin."

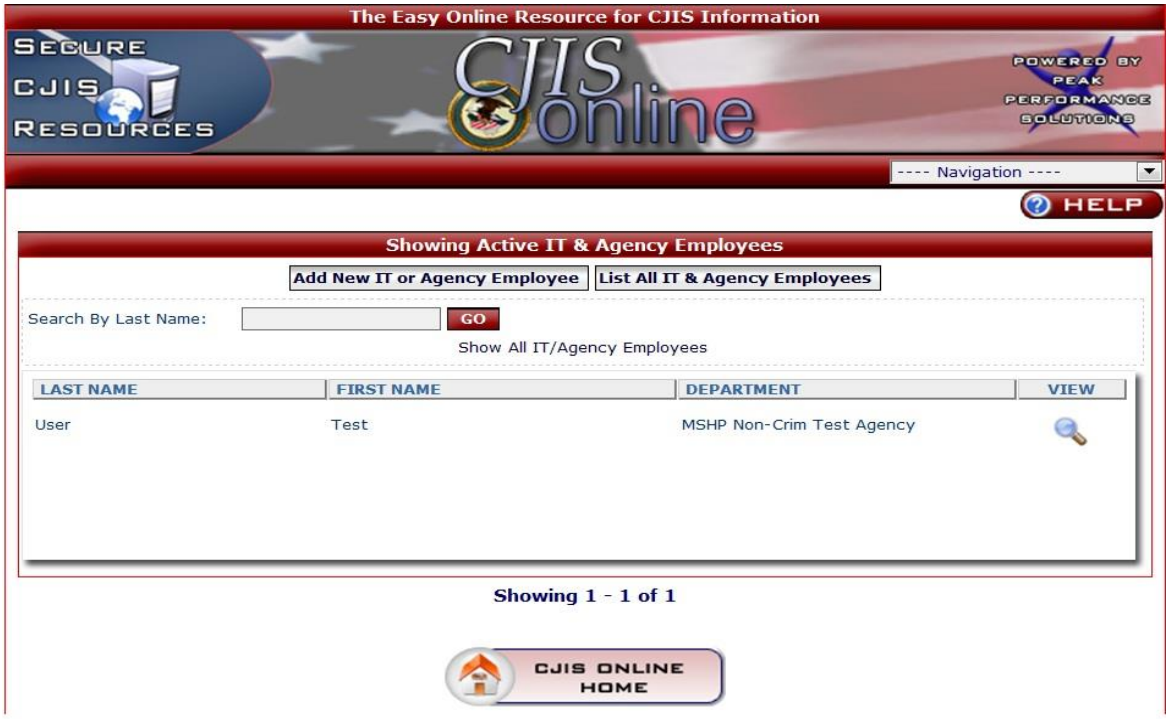
Enter your User ID and password. We recommend that you change your password after your initial login.



Select "IT & Agency User Admin" and click enter.



Adding an agency employee: Click on "Add New IT or Agency Employee."

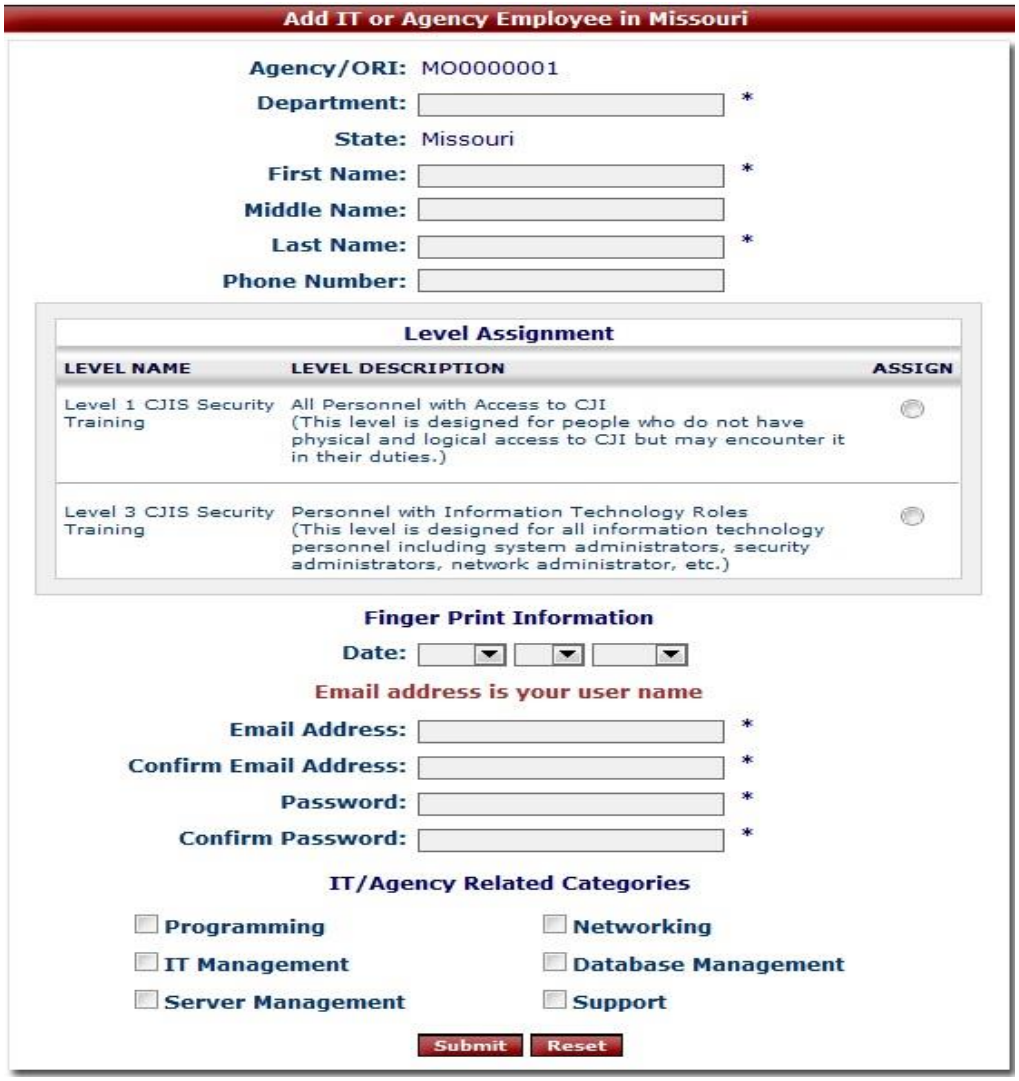


Fields with an * are mandatory.

The agency may enter the date the employee fingerprints are on file.

The agency will create the User ID and password for the employee.

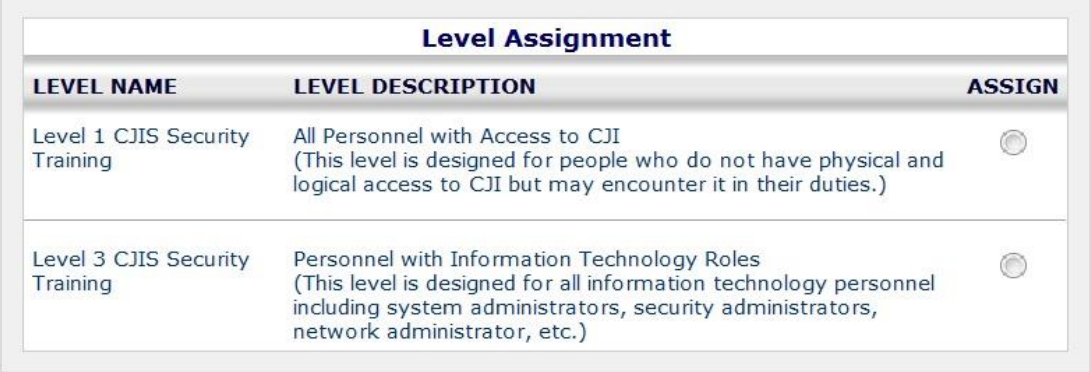
The email address of the employee will serve as their User ID.



Security Levels:

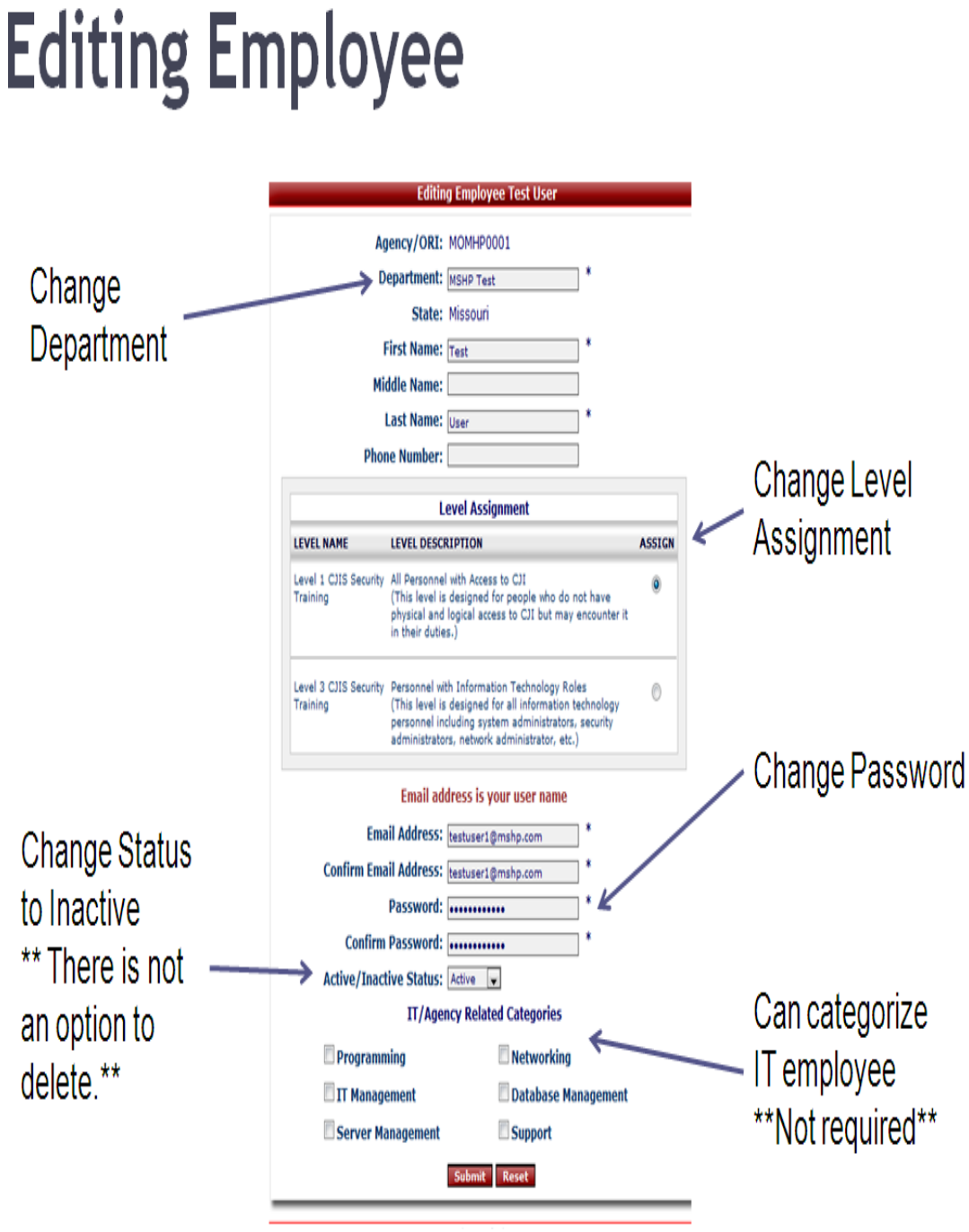
- Level 1 Employee Examples include: POC, Entity Head, Secretary, Mail Clerk, HR Manager, etc.
- Level 3 Employee Examples: IT Manager, IT Tech, Network Administrators

Most agencies will use the Level 1 access for Security Awareness Training.



Employee Profile — To view the employee profile, click on the magnifying glass located on the right of the employee name.

To edit, click on the red tab "Editing Employee."

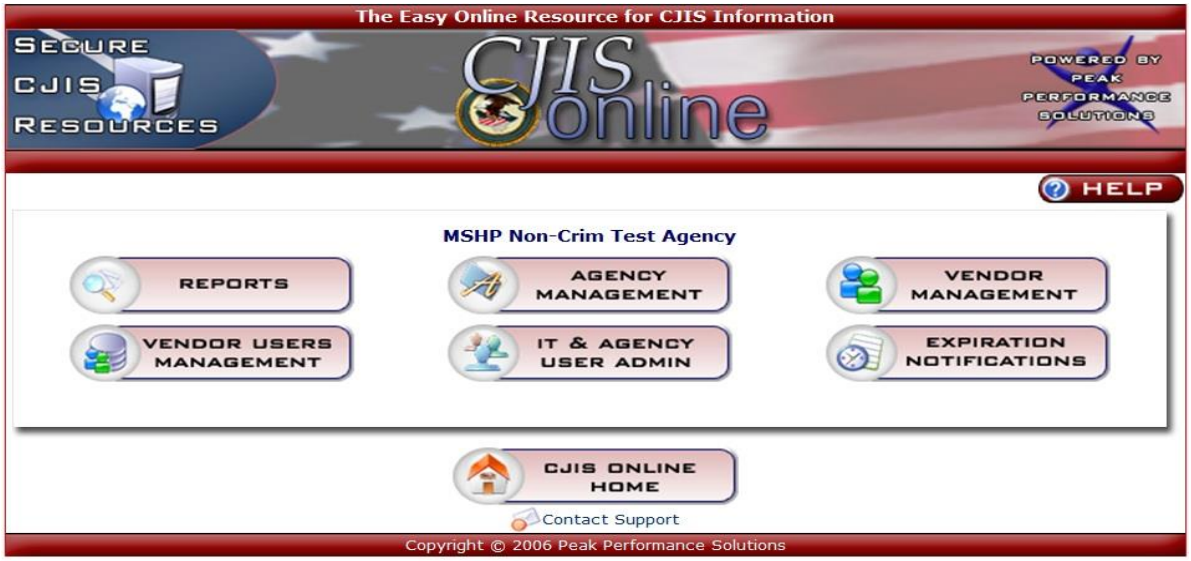


The agency can edit the employee information from this screen.

This screen is where the agency tracks an employee's testing history & fingerprint information.

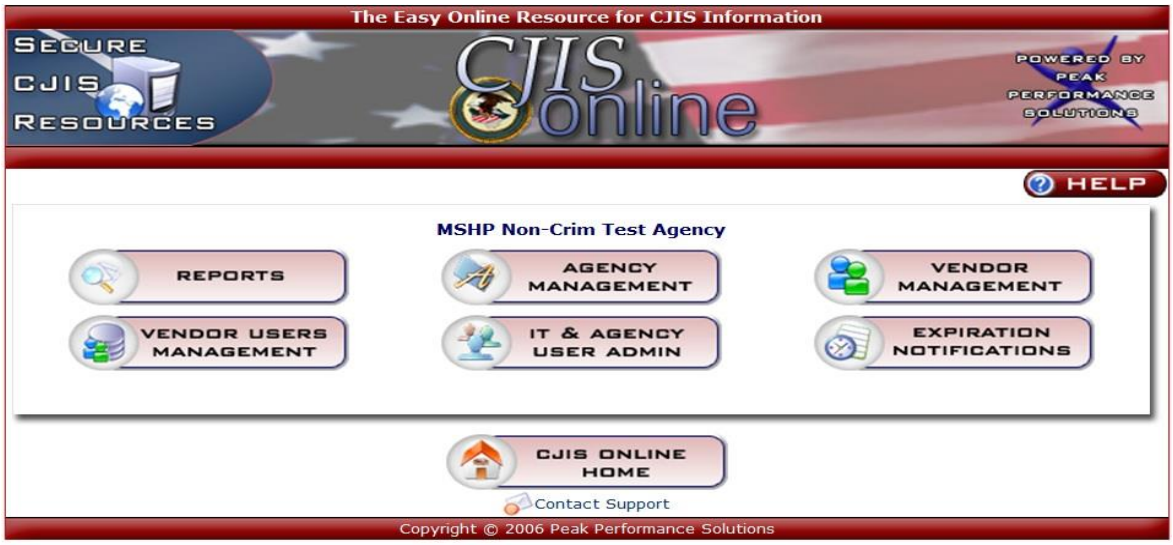
Use the "Navigation" drop down menu to return to the agency homepage and select other options. DO NOT CLICK ON "CJIS ONLINE HOME" UNLESS YOU ARE READY TO EXIT. Selecting this icon will log you out.

Agency Homepage — to select other options



DO NOT SELECT CJIS ONLINE HOME, IT WILL LOG YOU OUT!! This icon is used when you are ready to exit.

Click on "Reports."



To view test activity, click on "Test Activity Report."

You can search by a specific month, timeframe, or by all dates.

To view certifications, you will need to click on the "Navigation" dropdown, click on "Reports" and then click on "Certification Expiration Report." The screens will look similar to the "test activity reports." You will be able to search by month, timeframe, or all dates.

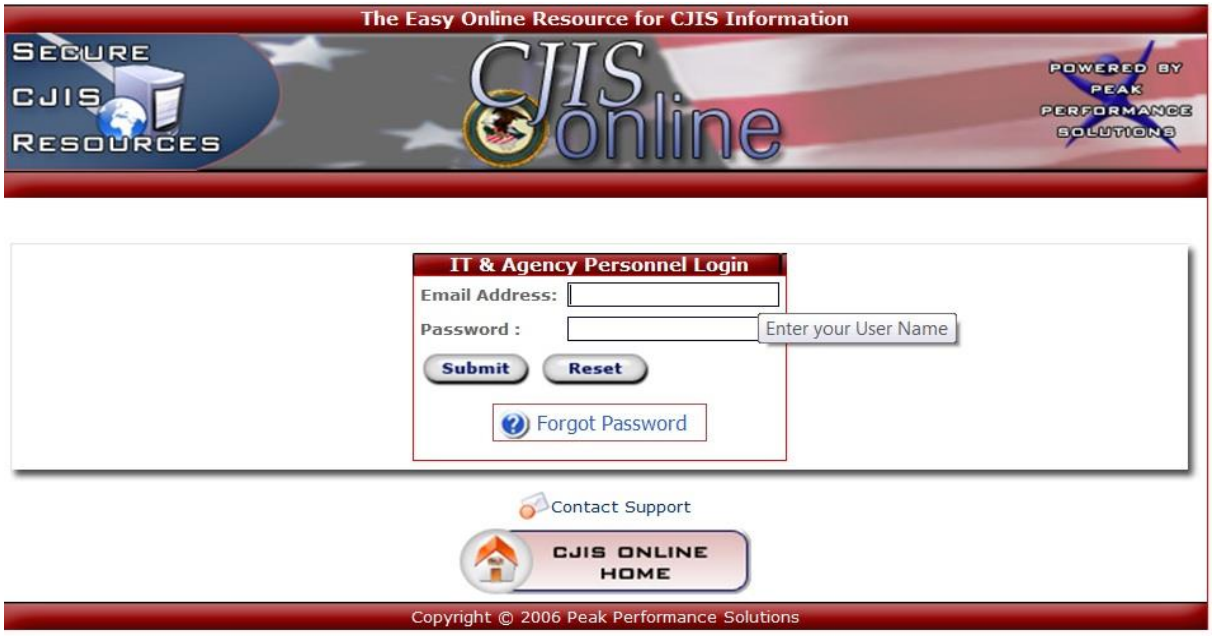
To view expiration notifications, you will need to go back to the agency homepage. Select the "Navigation" dropdown. From the dropdown, select "Expiration Notifications."

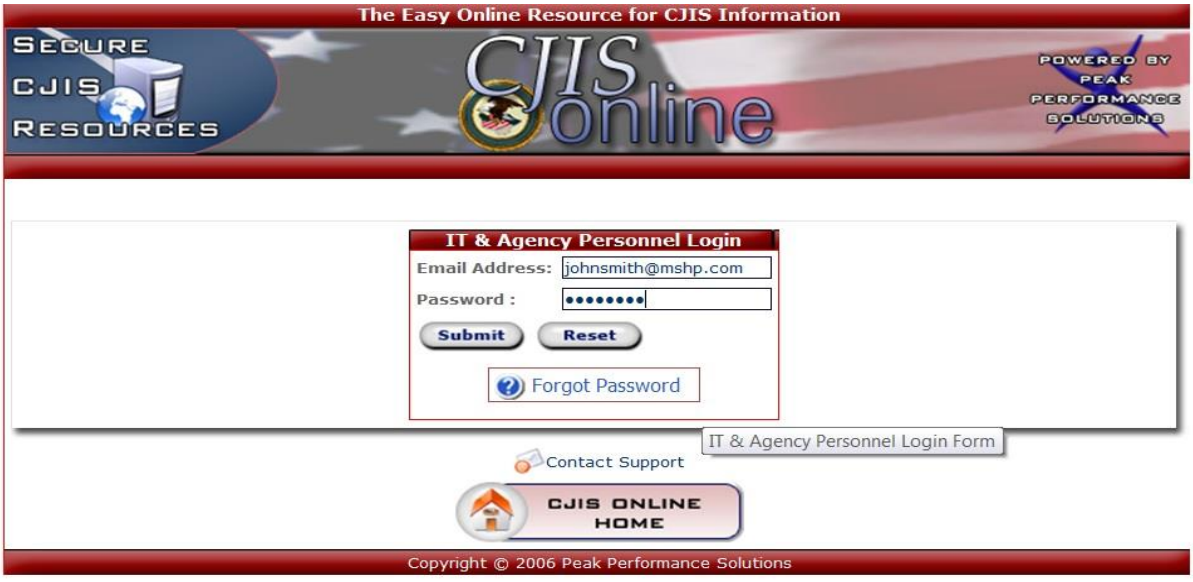
By placing a "check mark" in the box after "IT Personnel Expiration Notification," and selecting "Submit," you will receive an email notification when the employee's certification has expired.

To return to the CJIS online homepage, click on the icon "CJIS Online Home."

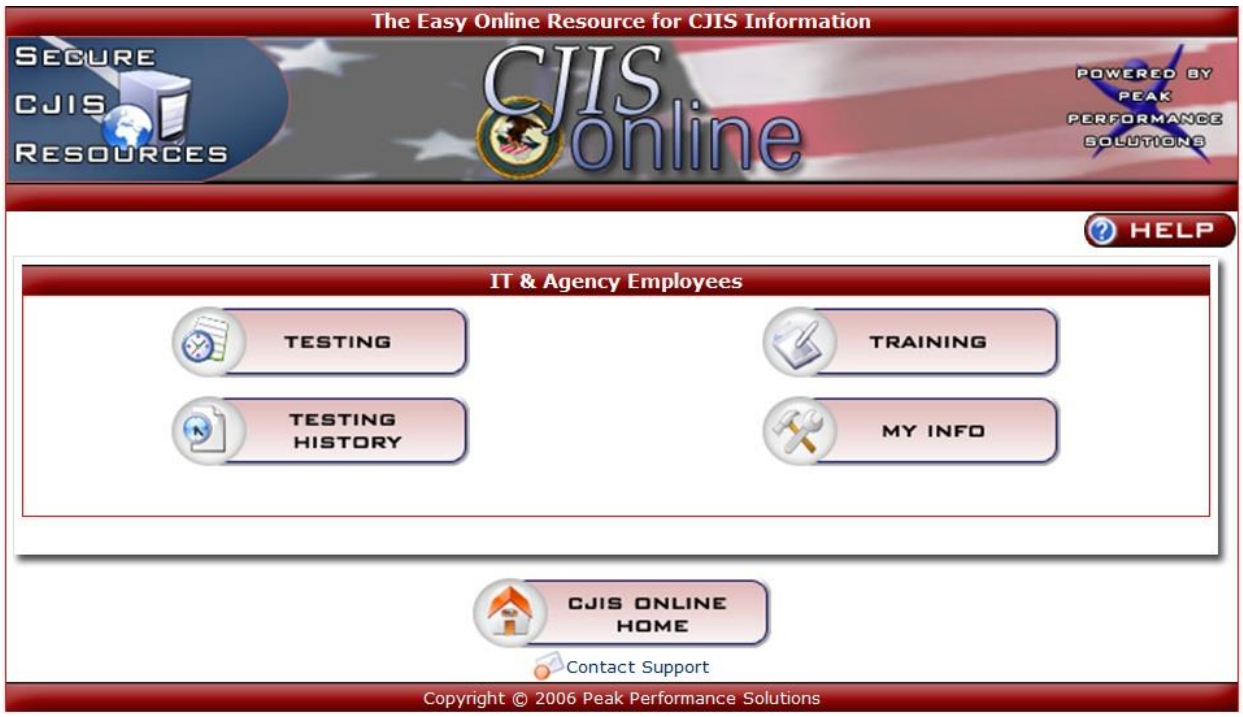
IT and agency user login: For employee use, the employee will select "IT & Agency Users."

The employee will receive their User ID and password from the agency/employer. The User ID will be the email address of the employee followed by a generic password, assigned by the agency/employer. The employee will enter their information and click on "Submit."



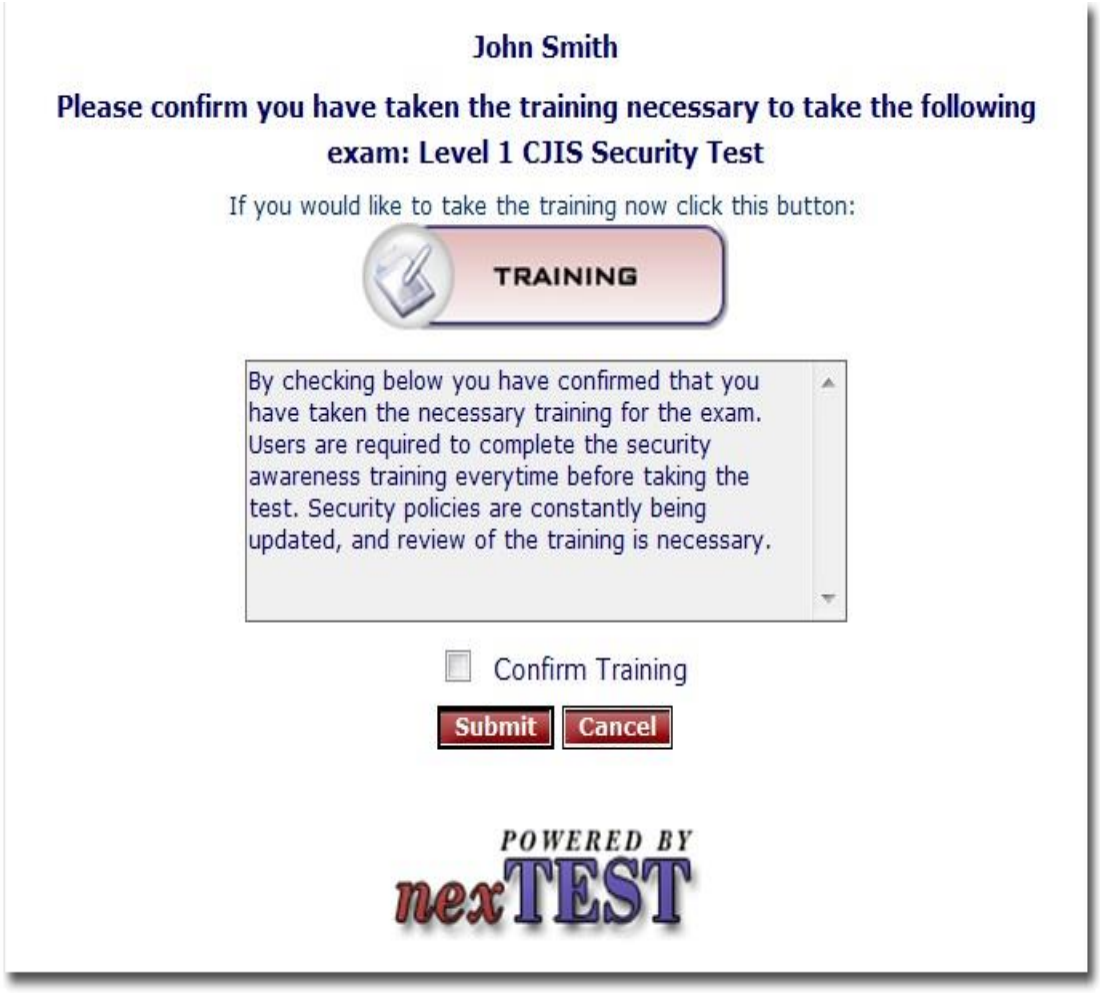


The IT and Agency Employee Page will look like this.



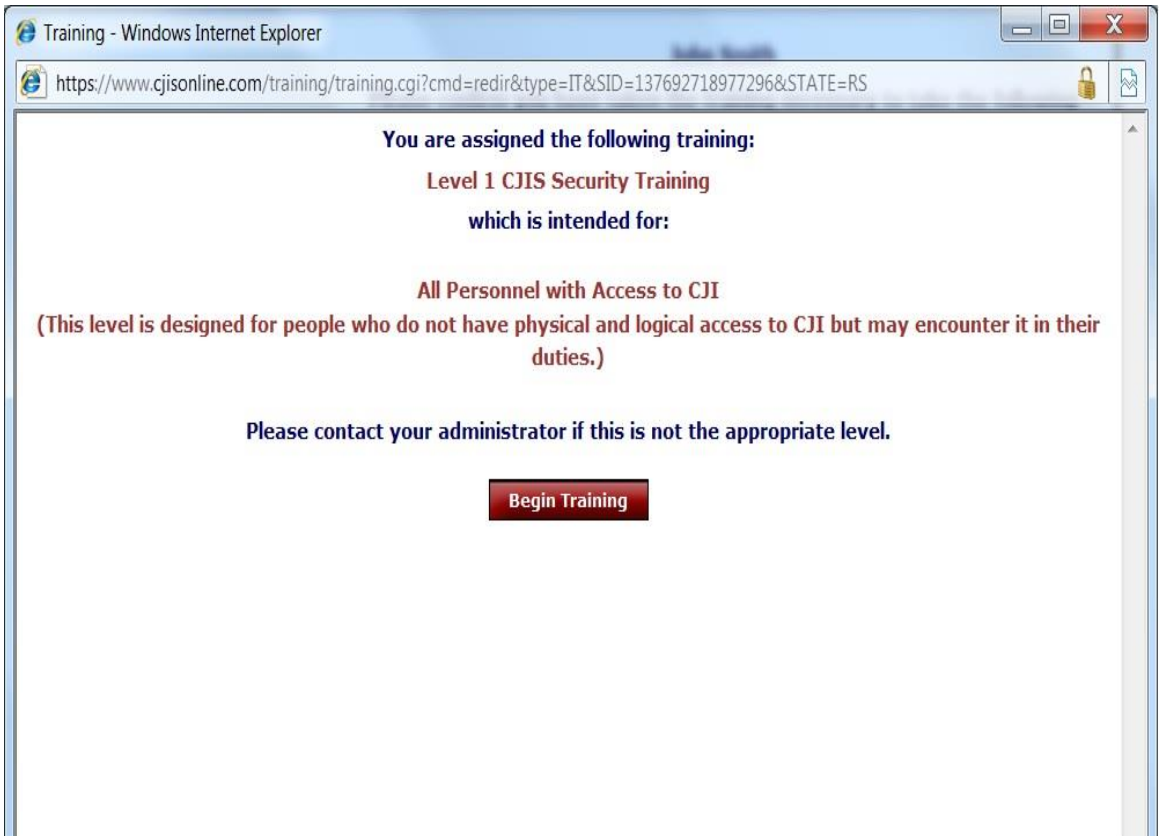
The icon, "My Info" is where the employee may make changes to their profile. It is recommended that the generic password is changed**.**

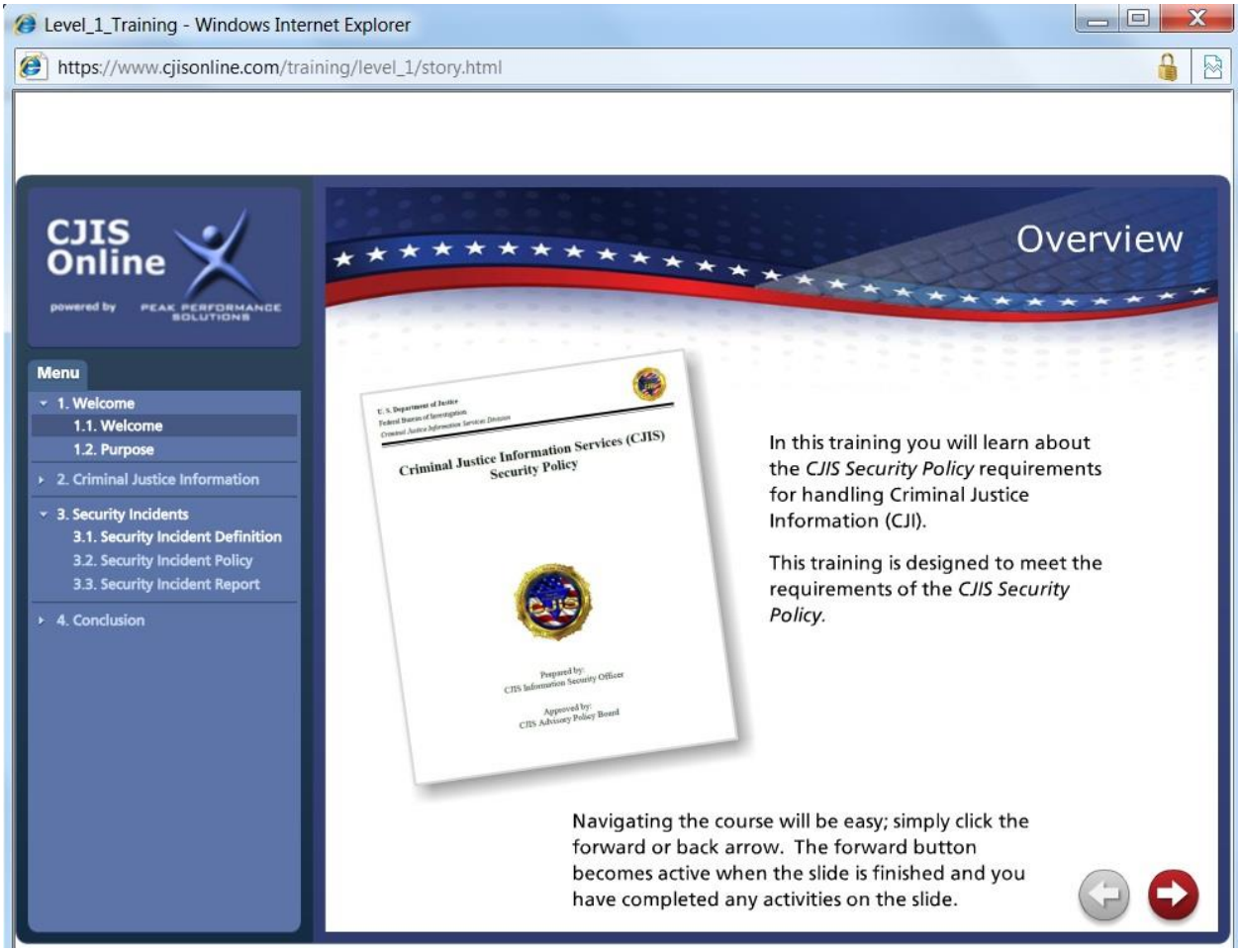
Click on the icon "TRAINING.” Upon completion of the training, you must confirm by placing a "check mark" in the box for "Confirm Training" and click on "Submit" tab.


John Smith
Please confirm you have taken the training necessary to take the following exam: Level 1 CJIS Security Test
If you would like to take the training now click this button:
TRAINING
By checking below you have confirmed that you have taken the necessary training for the exam. Users are required to complete the security awareness training everytime before taking the test. Security policies are constantly being updated, and review of the training is necessary.
Confirm Training
Submit
Cancel
POWERED BY
nexTEST

To begin the training segment, the employee will be directed to the screen below. Click "Begin Training."

The training segment will be specifically developed according to the access level the employee is assigned. Most employees will fall under LEVEL 1 CJIS Security Training.





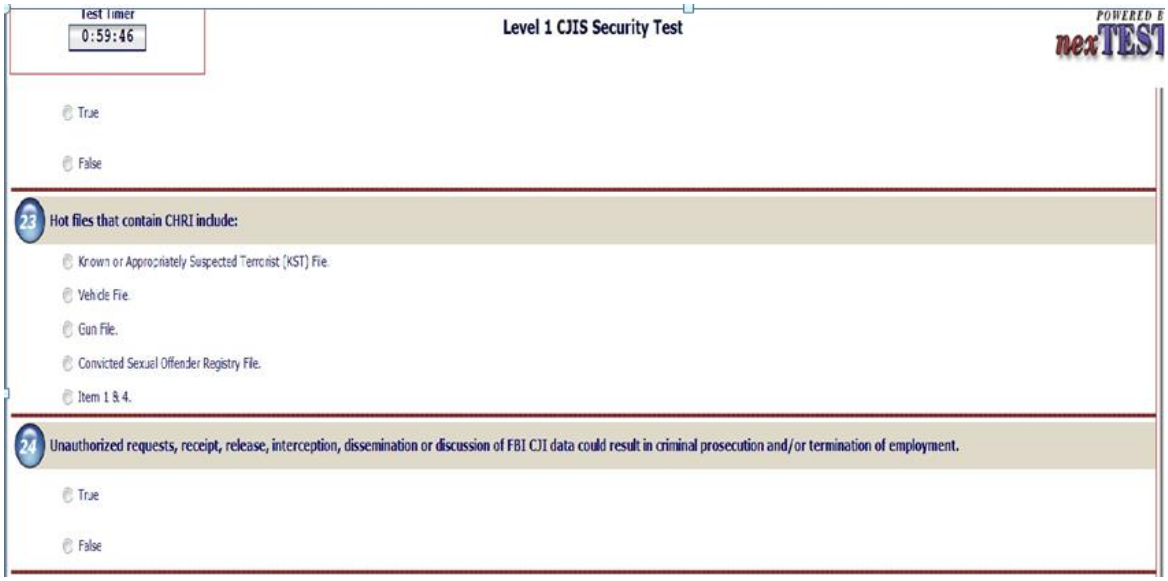
Navigating the course will be easy. Simply click the forward or back arrow. The forward button becomes active when the slide is finished and you have completed any activities on the slide. The training course can also be navigated by using the side bar, under the Menu tab. You may click on the section in which you would like to view.

When training is completed, place a "check mark" in the box for "Confirm Training.” Click on "Submit" to continue.

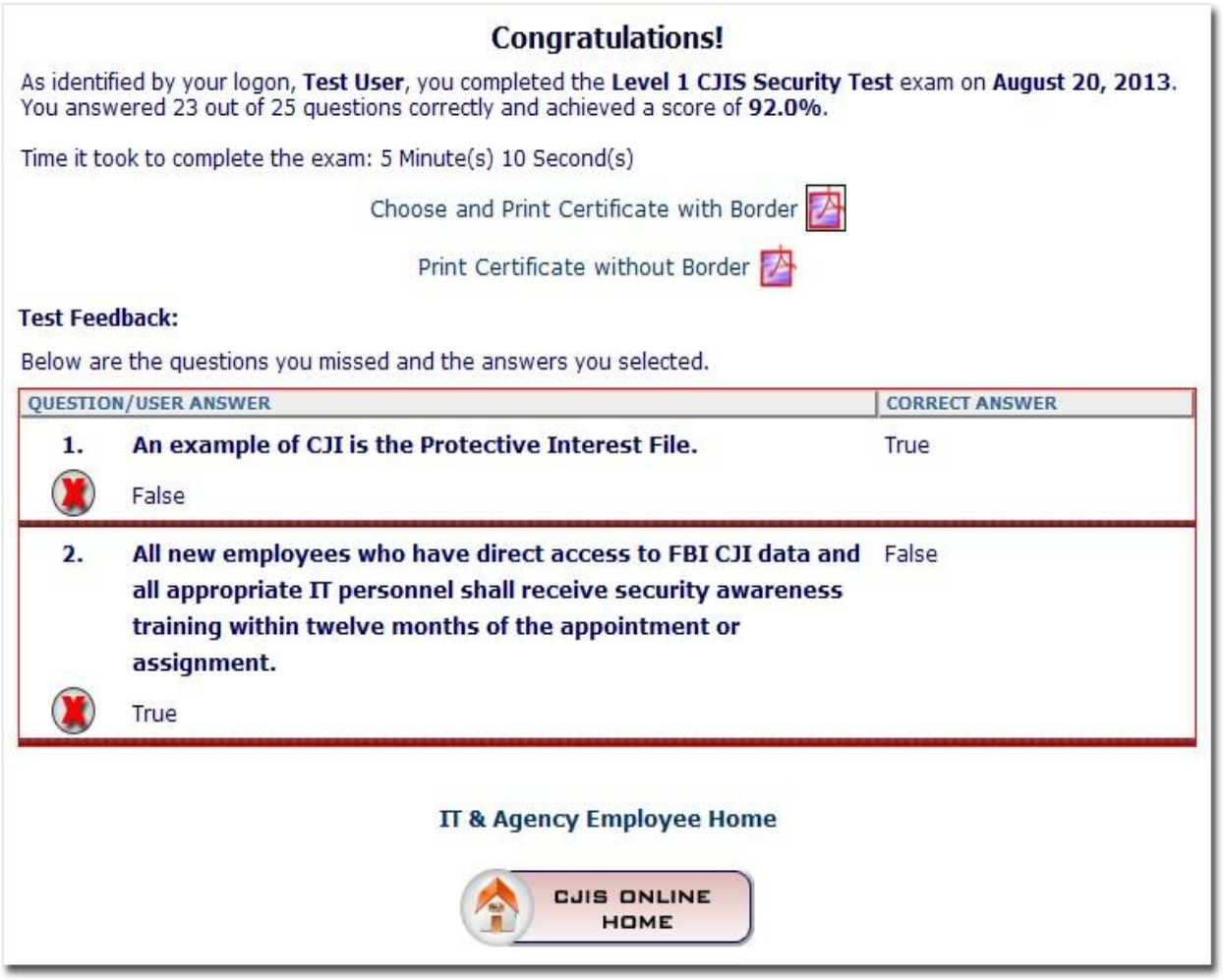
After confirming the training has been completed, the employee will be directed to the test.

The testing confirmation page will appear similar to this. The employee will need to click on the icon "Continue" to begin the testing.

Example of a test page.



Upon completion of the test, the employee will be notified immediately of the results. For successful completions, the employee will have the option of printing a certificate of completion. The employee may click on the icon "Choose and Print Certificate with Border" or "Print Certificate without Border."



Congratulations!

As identified by your logon, **Test User**, you completed the **Level 1 CJIS Security Test** exam on **August 20, 2013**. You answered 23 out of 25 questions correctly and achieved a score of **92.0%**.

Time it took to complete the exam: 5 Minute(s) 10 Second(s)

Choose and Print Certificate with Border

Print Certificate without Border

Test Feedback:

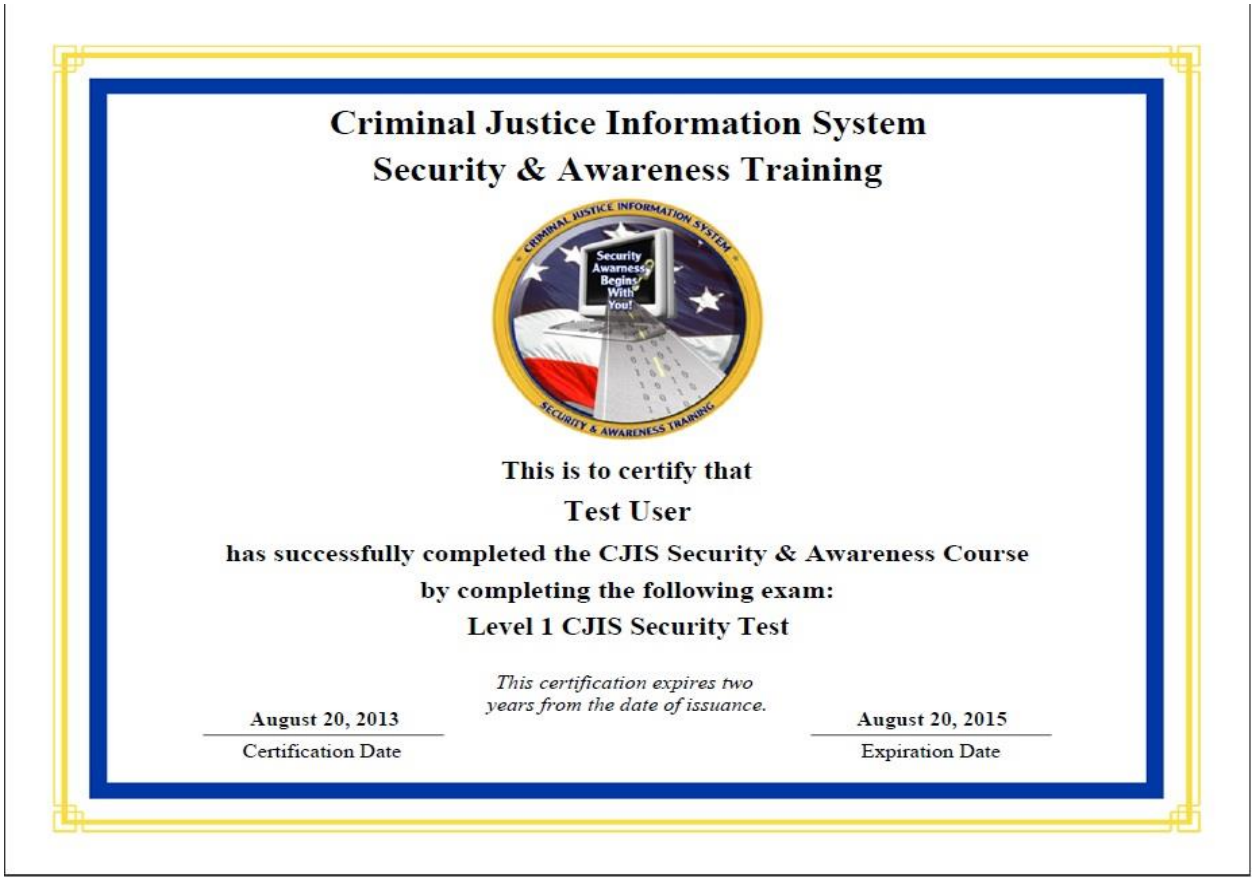
Below are the questions you missed and the answers you selected.

QUESTION/USER ANSWER	CORRECT ANSWER
1. **An example of CJI is the Protective Interest File.**	True
False	
2. **All new employees who have direct access to FBI CJI data and all appropriate IT personnel shall receive security awareness training within twelve months of the appointment or assignment.**	False
True	

IT & Agency Employee Home

CJIS ONLINE HOME

Certificate Example:



Criminal Justice Information System
Security & Awareness Training

This is to certify that

Test User

has successfully completed the CJIS Security & Awareness Course
by completing the following exam:
Level 1 CJIS Security Test

This certification expires two years from the date of issuance.

August 20, 2013	August 20, 2015
Certification Date	Expiration Date

Return to IT and Agency Employee Home, Select "Testing History."

Testing history will provide testing information of the user. In additional to showing the test date and pass/fail with score, the employee may print a certificate from this screen.

Reminders:

If the USER forgets their password, the LASO (local agency security officer) can edit or reset the password.

If the LASO forgets their password, they must contact the MSHP-CJISD Security Unit, or

MSHP-CJISD Auditor/Trainers: (573) 526-6153

- Ms. Pam Aberle, ext. 2625
- Ms. Linda Lueckenhoff, ext. 2630
- Ms. Valerie Hampton, ext. 2655
- Mr. Scott Schlueter, ext. 2653

SECTION 6: POLICY COMPLIANCE REVIEW (AUDITS)

6.1 Background

The CJIS Security Policy provides the minimum standard requirements for states to follow. The states, by policy, may adhere to the minimum standards or choose to be more restrictive, but they cannot be less restrictive. In December 2002, the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) recommended that the FBI CJIS Audit Unit begin auditing Noncriminal Justice Agencies (NCJAs) that receive FBI criminal history record information via applicant fingerprint processing. The FBI CJIS Audit Unit began conducting pilot audits on these agencies in 2004, and in October 2008, began to permanently conduct noncriminal justice agency audits.

With this new requirement, the APB approved a section in the CJIS Security Policy to include a state requirement to audit noncriminal justice agencies with indirect access to III system information. The requirement stated:

"The appropriate, authorized state official, which may be the CJIS systems officer, the state compact officer, or the state repository director, shall periodically conduct audits of the state's noncriminal justice agencies with indirect access to III information through the submission of fingerprints." (U.S. Department of Justice, FBI, *Informational Letter Regarding State Noncriminal Justice Agency Audits,* dated Feb. 9, 2009.)

The FBI CJIS Security Policy, Appendix J requires that "states shall periodically conduct audits of NCJAs. The FBI CJIS Division shall triennially conduct audits of a sampling of NCJAs."

In addition, CSAs shall, in coordination with the State Identification Bureau (SIB), establish a process to periodically audit all NCJAs with access to criminal justice information in order to ensure compliance with applicable statutes, regulations, and policies.

In Missouri, the process of periodically auditing all NCJAs with access to criminal justice information (CJI) is the responsibility of the MSHP-CJISD. Thus, in 2009 and in response to the APB, the MSHP-CJISD developed the noncriminal justice audit program with designated NCJA auditors. The NCJA audits, referred to as policy compliance reviews (PCRs), are conducted with each agency on a triennial basis. Generally, the first PCR is conducted within the first year of access and triennial thereafter. Reviews may be conducted more frequently than the standard three years, and an agency may request a review any time the point contact believes it would be beneficial to their agency. Such requests should be directed to the regional CJIS auditor/trainer.

6.2 Areas Of Review

- Local Agency Security Officer/Point Of Contact
- User Agreement
- Use & Access Of CHRI
- Fingerprint Submission Policy
- Dissemination Practices/Policy
- Retention/Storage Policy
- Destruction Policy
- Waiver Agreement & Statement (VECHS only)
- Security Awareness Training
- Outsourcing

6.2.1 Local Agency Security Officer & Point Of Contact — The LASO and POC may be the same person within the agency. Per the CJIS Security Policy, the LASO must be a full-time employee of an agency unless the agency is deemed a part-time agency.

6.2.2 User Agreement — Per the CJIS Security Policy, each agency with access to CJI must have a current and valid user agreement.

A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. attorney general. A NCJA (public) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board.

A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (private) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access.

All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy. (See Appendix J for supplemental guidance). Each NCJA that directly accesses FBI CJI shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system per authorization of Department of Justice (DOJ) Order 2640.2F.

6.2.3 Use & Access Of CHRI — An agency will be assessed for compliance regarding the use and access to the CHRI. Compliance assessment includes the verification that the agency is using the CHRI for the purpose for which it was obtained. The purpose and use must be in accordance with the authority of the

agency. The authority is based on the ORI approval and the state or federal law that granted access to CHRI.

Access to CHRI is based on fingerprint submission and is tracked by the MSHP-CJISD with dissemination logs for an agency ORI or ORI and OCA. The fingerprint submission (or data sampling) will show a list of records that the requesting agency has received. The data sampling may include 25 record requests and may include a timeframe from the previous three years to the current date. An additional sampling beyond 25 records is authorized if deemed necessary.

Generally, PCRs are scheduled with the agency approximately six weeks in advance; however, the MSHP-CJISD reserves the right to make unannounced visits.

Things to consider regarding access to CHRI:

1. Is the criminal history record being requested on an individual affiliated with the requesting agency and for an authorized purpose, i.e., employment, volunteering, licensing?
2. Does the purpose match the authority identified in the state law or federal law?
3. If the agency is a VECHS agency, was the applicant given the Waiver Agreement and Statement prior to being asked to submit fingerprints? Is the agency retaining a copy of the signed waiver?
4. Is the criminal history response from the MSHP/FBI being disseminated to another agency or person? Before granting access through dissemination, you must first ensure that access or dissemination is authorized. Please remember, access can be in many forms, i.e. verbal, written, electronic, email, or facsimile, and must be authorized.

Reminder: Any use of CHRI outside of the authorized purpose as stated in either state statute or the federal law is strictly prohibited and may be deemed as "misuse" and is subject to state and federal criminal and civil penalties.

6.2.4 Fingerprint Submission Practices — Each agency should have a policy or procedure in place for fingerprint submission practices. The MSHP accepts both hard copy fingerprint cards and electronic fingerprint image and data submission. Although both methods of submission are acceptable, they both have very different submission requirements. (Please see Section 8 for more information about fingerprint submission.)

To help prevent the possibility of applicants that have a criminal history asking someone else without criminal history to pose as the applicant for fingerprinting purposes, it is recommended to request and obtain photographic identification when capturing an individual's fingerprints. Do not provide the fingerprint card to the applicant to submit to the MSHP, as the applicant could alter the card.

It is recommended that agencies accept only current, valid, and unexpired photo identification documents. As a primary form of picture identification, an applicant may present a state-issued driver's license, which meets the requirements of Public Law 109-13, Title II, Section 200, when being fingerprinted. Other forms of secondary documents, in part, include a state identification card, state government issued certificate of birth, U.S. active, retired, or reservist Military ID, U.S. passport. When validating the authenticity of secondary identification documents and forms, the data and information

may be supported by at least two of the following: utility bill, jurisdictional voter registration card, vehicle registration card or title, paycheck stub with name and address, jurisdictional public assistance card, spouse or parent affidavit, canceled check, bank statement, or mortgage documents. When an agency has a reason to believe an applicant has presented fraudulent information, agency personnel should contact local law enforcement.

6.2.5 Suggested Chain Of Custody Procedures For Fingerprints — An agency may employ a process to protect the integrity of the applicant's fingerprints when they are forwarded to the Central Repository (MSHP). The following information provides a guide to developing a chain of custody process:

- Establish provisions for the agency to manage both manually and electronically captured fingerprints.
- Establish an agency tracking system or applicant log using the employee's name or some other method for identifying the individual capturing the fingerprints and verifying the applicant's identity.
- Establish a procedure that documents the type of identification used by the applicant.
- Establish procedures that use special sealed envelopes, agency specific stamps, etc., for the agency to use when forwarding the applicant's manual fingerprint card.
- Implement the use of forms that may include the date of fingerprinting, reason, the name of the applicant, etc.

6.2.6 Dissemination Practices — Each agency will be assessed on dissemination practices. For agencies that allow dissemination to another agency (subject to authorization), or to the subject of record, procedures must be followed to ensure compliance with state and federal law. For this reason, each agency should have a policy or procedure in place outlining their dissemination practices, if any.

6.2.7 Retention & Storage Policy — Each agency will be assessed on retention practices. CJI may be destroyed at which time it is no longer needed. CJI is not needed for audit purposes since the MSHP-CJISD keeps a dissemination record of all CJI disseminated to all agencies.

For audit purposes, the agency is required to keep supporting documentation that substantiates the legal authority or purpose for requesting the CJI (i.e. an employment application, applicant file, waiver form, or some other type of document that proves the applicant applied for, retained a position at, or received some type of benefit from the agency.) If unable to provide supporting documentation, the request for CJI may be deemed as unauthorized.

If your agency policy is to retain the CJI, it must be kept in a secure records environment and free from public or unauthorized access. The area must be secured by lock and have limited access. If CJI is retained in electronic media, the data must be protected and not accessible from outside the agency or across state lines. If storage of CJI is off-site and under the control of a third party, the agency will be required to obtain an Outsourcing Management and Control Agreement prior to allowing a third party access or storage responsibilities of the CJI. (See current Outsourcing Standard.)

6.2.8 Destruction Policy/Practices — Each agency will be assessed on destruction of CJI, if destroyed. It is recommended that destruction be completed on-site at the agency by authorized agency personnel and in a manner that is acceptable to CJIS Security Policy. If your agency contracts with a private destruction company, the destruction must take place under your agency's direct supervision. If any agency allows destruction of CHRI to occur off-site, an Outsourcing Management and Control Agreement is required prior to access. (See current Outsourcing Standard.)

6.2.9 Waiver Agreement & Statement — (VECHS agencies only) — The Waiver Agreement & Statement (SHP-981) is a form required by all VECHS agencies only. The Missouri VECHS program is a MSHP program approved by the FBI through federal legislation and administered by the CJIS Division. The VECHS program is not in Missouri state law and not approved pursuant to Public Law 92-544; therefore, the approval of the VECHS program through federal law requires the use of a waiver. The Waiver Agreement & Statement adheres to the FBI requirement of Title 28, 16.30-34 and is auditable. Each VECHS entity is required to produce the waivers during the PCR. Failure to obtain waivers from the applicant prior to requesting CHRI may subject the agency to civil liabilities. For audit purposes, the agency may be assessed as noncompliant, which may require a follow up audit and could also result in suspension of access to CHRI.

6.2.10 Security Awareness Training (SAT) will be reviewed to ensure individuals with access to CJI have completed the required training. Basic SAT is required within six months of initial assignment, and biennially thereafter. Access to CJI includes direct access or access to CJI through fingerprint submission. SAT is available online with training and testing. (Refer to Section 5 for more information.)

6.2.11 Outsourcing will be discussed with the agency to ensure agency personnel are aware of what constitutes as outsourcing. When an agency is allowing a third party to have access to CJI in any form, the agency must have an approved outsourcing standard in place.

Some examples of unauthorized outsourcing include:
1. Allowing a third party to handle destruction off-site or unsupervised;
2. Storing agency files containing CJI off-site under the control of a third party;
3. Retaining electronic CJI on a server that is accessible by third parties;
4. Contracting with a third party for administrative services to view and make eligibility determinations.

6.3 PRE-REVIEW PREPARATION PROCESS FOR PCRs

The CJIS auditor will review the agency information and contact the agency POC approximately six weeks prior to the on-site review to gather or confirm basic information regarding the agency's use of CHRI. During this initial contact, the reviewer will answer any agency questions concerning the review process, discuss logistics pertaining to the on-site visit, and make preliminary plans regarding the review. The CJIS auditor will follow up with written confirmation of the date and time of the scheduled review to the entity head/representative or POC.

6.4 ON-SITE AGENCY REVIEW PROCESS

6.4.1 Administrative Interview At the pre-arranged time, the CJIS auditor will conduct the on-site portion of the agency review. During this portion, the POC should be present. The administrative interview is used to determine whether agency CHRI policy and procedures for receipt of state and FBI criminal history are in accordance with state and federal law.

6.4.2 Data Quality Review. In conjunction with the interview, a data quality review is conducted. During the data quality review, records are checked for factors including authorized request, purpose, retention, destruction, security, and dissemination. Records with errors are documented for evaluation and appropriate action by the agency POC or agency representative. Noncompliant records are classified into one or more of the following categories:

- ***Unauthorized Request*** — CHRI was requested without legal authority; requesting CHRI for another purpose outside the scope allowed in statute or law; failing to provide supporting documentation to auditor that substantiates the request for CHRI.

- ***Unauthorized Dissemination*** — CHRI disseminated to an unauthorized person or agency; CHRI disseminated out of state; CHRI stored on a company server or website that is accessible to others not authorized to view.

- ***Unsecure Location For CHRI*** — CHRI maintained in open cabinets; CHRI maintained electronically without proper technical safeguards; CHRI stored electronically or in hard copy form in an unrestricted environment.

- ***Fingerprints Not Submitted*** — This category is applicable to agencies required by state or federal law to submit fingerprints on applicants for specific purposes, i.e. concealed carry permits, housing applicants, emergency child placements.

- ***Failure To Submit Fingerprints In A Timely Manner*** — This category specifically applies to the DSS Children's Division for emergency child placements.

6.4.3 Exit Briefing The purpose of the exit briefing is to present the findings of the review to the POC or agency representative. The formal summary and findings document may be left with the agency at the time of the PCR, or the CJIS auditor may complete the findings and electronically send the document to the POC or agency representative at a later date. Generally, the electronic summary and findings document is sent via email to the agency POC within 10 business days following the completion of the review. The CJIS auditor may require a follow-up audit within 60-90 days to address any areas of concern, or those items deemed noncompliant. If the areas of concern have been satisfied during the follow-up review, no further action will be required.

6.5 Agency Requirement For Noncompliance Findings

For all areas of concern or those deemed noncompliant, the agency POC is required to provide a written response to the MSHP-CJISD within 30 days after the PCR completion date, addressing noncompliance areas. The response letter should include a plan of action that will place the agency within policy guidelines.

Upon completion of the corrective measures, the agency head or POC must notify the MSHP-CJISD in writing that the agency has accomplished its planned objectives and is now in full compliance with policy and regulations.

If the agency POC fails to provide the MSHP-CJISD with a plan of action, the agency will be considered noncompliant and will be subject to suspension of access to CHRI.

If an agency refuses to cooperate in an agency/MSHP-CJISD audit, the agency will be considered noncompliant and access to CHRI will be suspended.

6.6 Survey —Using Survey Monkey

The final part of the PCR process is the survey. Each agency will have an opportunity to complete a survey after the PCR process is complete. The survey is an online link which will be sent via email to the agency POC. Through Survey Monkey, an agency can access the site and complete a brief survey. The survey also provides areas for additional comments, inquiring as to any areas of the PCR that were most and least beneficial. While the survey itself is optional, for those that choose to participate, the agency name is optional for anonymity. The responses collected from the survey are used to ensure the PCR process is beneficial and may also help to identify any areas of concern or training needs.

SECTION 7: SECURITY & MANAGEMENT CONTROL OUTSOURCING STANDARD

To assist agencies with outsourcing, this section provides a summary of the requirements and responsibilities of both the authorized recipient and contractor. The provisions of the Security and Management Control Outsourcing Standard (Outsourcing Standard) are established by the Compact Council pursuant to Title 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the authorized recipient to perform noncriminal justice administrative functions requiring access to criminal history record information without a direct connection to the FBI CJIS Wide Area Network.

As a summary, the information contained in this section is not all inclusive and agencies are instructed to read, in full, the Outsourcing Standard document. A complete copy is available in Appendix E of this manual, along with links to the MSHP and FBI website.

7.1 What Is Outsourcing?

Outsourcing is a term heard frequently in recent years referring to the delegating of a function to an independent provider. In the realm of criminal justice, this refers to a specific type of outsourcing that involves access to confidential and restricted information obtained from the systems of the MSHP and FBI.

Authorized recipients of criminal history record information may have the need to outsource some responsibilities to an outside agency or third-party contractor. In terms of outsourcing duties as they relate to criminal history record information, this may include an authorized recipient contracting with a third party to review the background check results and make the eligibility or hiring determinations, storage of personnel files containing criminal history records, and destruction procedures. In addition to hard copy access to criminal history records, outsourcing also applies to electronic media. There is an increasing occurrence of record information being maintained electronically and accessed by information technology vendors and contractors.

Prior to allowing a third-party contractor access to criminal history records, an Outsourcing Standard must be approved by the MSHP-CJISD and state compact officer.

Outsourcing of noncriminal justice administrative functions from the authorized recipient to a contractor includes, but is not limited to, the following:

1. Making fitness determinations and/or recommendations,
2. Obtaining missing dispositions,
3. Disseminating CHRI as authorized by federal statute, federal executive order, or state statute, and

4. Other authorized activities relating to the general handling, use, and storage of CHRI.

7.2 What Is An Outsourcing Agreement? When Is It Needed?

The National Crime Prevention and Privacy Compact Act of 1998 established the infrastructure that allows states to share information for noncriminal justice purposes. It also created the Compact Council which serves as the governing body that establishes the rules and procedures regarding access to III.

Criminal history record information is confidential and must be protected from creation through destruction. In order to address issues of outsourcing, the Compact Council enacted the *Security and Management Control Outsourcing Standard for Non-Channelers.* The purpose of the Outsourcing Standard, in part, is to provide adequate security and integrity for criminal history record information while under the control or management of an outsourced third-party, the contractor. It also requires the contractor have in place the proper security program that will ensure the integrity of information obtained is not compromised and meets all requirements of state and federal laws, FBI CJIS Security Policy, and the United States attorney general.

To ensure the contractor adheres to all security procedures as required under the Outsourcing Standard, the authorized recipient must enter into a contract with the third-party contractor specifying the exact duties of the contractor as outlined in the Outsourcing Standard document.

7.3 Responsibilities Of The Authorized Recipient

The contractor must not have access to criminal history record information until an approved Outsourcing Standard is in place. When a third party contractor is to perform any duties requiring access to criminal history record information, the authorized recipient shall:

1. Specify the terms and conditions of access.
2. Limit use of information for the sole purpose intended.
3. Limit retention of CHRI not to exceed the retention period of the AR.
4. Prohibit dissemination, unless authorized.
5. Ensure security and confidentiality of CHRI.
6. Provide for audits and sanctions of the contractor.
7. Provide for conditions of termination of contract.
8. Conduct background checks for contractor personnel. The AR is required to conduct criminal history background checks of the contractor's personnel who have access to CHRI, if this is required by the AR's personnel with the same level of access. The AR is to maintain accurate and current records of contractor personnel who have access to CHRI.
9. Ensure that the contractor maintains site security and there is no unauthorized access to CHRI.
10. Conduct an audit of the contractor within 90 days from the date that the contractor has received CHRI under the agreement.
11. Have a good knowledge of the contractor's communications and record capabilities and maintain an updated topological drawing of the contractor's network configuration.

12. Provide written notification to the state compact officer of any early voluntary termination of the contract.

7.4 Responsibilities Of The Contractor

1. Security Program Requirement — In addition to complying with all federal and state laws and other regulatory authorities, including the Compact Council, the contractor must implement a Security Program. The Security Program makes up a very significant portion of the contractor's responsibilities, as it addresses nearly all areas of the contractor's security as it relates to their outsourcing function: physical site security, personnel security, and information technology. The Security Program should contain, at a minimum:
    - Description of the implementation of the security requirements pursuant to the Outsourcing Standards and the CJIS Security Policy.
    - Security Training for contractor personnel. A Security Training Program is to be reviewed and approved by the AR prior to any access or assignment of contractor personnel that involves access to CHRI. Training will be required upon any change in federal or state laws, regulations, or any as established by the Compact Council or United States attorney general. Annual refresher training should also be provided.
    - Guidelines for the documentation of security violations.
    - Standards for the selection, supervision, and separation of personnel with access to CHRI.
2. Audit Requirements — Contractor shall make its facilities available for both announced and unannounced audits on behalf of the AR, the state, or the FBI on behalf of the Compact Council. The contractor's Security Program is also subject to review by these same authorities. As stated earlier in the AR's responsibilities, the contractor is subject to a mandatory review within the first 90 days from the date that the contractor first receives CHRI.
3. Retention Period for CHRI — The contractor may only retain CHRI for an amount of time that is necessary to fulfill terms of the contract and should not exceed that of the retention period of the AR.
4. Dissemination of CHRI —
    - Contractor shall not disseminate CHRI without the consent of the AR and must be specifically authorized by state and federal laws, regulations and standards, and in accordance to Compact Council policies and procedures.
    - Contractor must keep a log of all authorized dissemination for a minimum of one year.
    - If stored electronically, the contractor must ensure that the equipment and data stored is protected against any unauthorized access.
5. Personnel Security —
    - The contractor's personnel shall be subject to the same background check requirements as the AR's personnel with similar access to CHRI. Criminal history record checks must be completed on contractor personnel before any access is given to CHRI under the contract.
    - The contractor must confirm that employees understand the Outsourcing Standard an all laws pertaining to the security and integrity of CHRI. Written certifications must be obtained from employees and kept on file with the contractor, and will be subject to review during audits.

- Current personnel records shall be maintained of those employees who have access to CHRI, which will include background screenings, if necessary. Contractor must keep a complete list of all personnel who have access to CHRI and update those records within 24 hours if any changes occur. The AR must also be notified of any access additions or deletions within 24 hours.

6. System Security — Most issues involving system security requirements under an outsourcing agreement are found within the CJIS Security Policy. If CHRI is accessible by unauthorized personnel via a Wide Area Network/Local Area Network or the Internet, the contractor will be required to protect the CHRI through the use of firewalls to prevent unauthorized access. Any CHRI that is transmitted through a shared public carrier network must utilize data encryption. The contractor must ensure secure storage, maintenance and disposal of all hard copy and electronic media. Please refer to the CJIS Security Policy for more information regarding security system requirements.
7. Security Violations — The contractor and the AR are both responsible for the handling of any security violations.
    - If the contractor suspects any violations have occurred, an employee must be suspended of their assignment as it related to their access to CHRI, pending any investigation.
    - The contractor is required to immediately report such security violations to the AR (within four hours) and to subsequently provide written documentation (within five days) as to the specifics of the incident and to include corrective actions to resolve the violation.
    - The AR is required to immediately (within four hours) report the security violation to the state compact officer and will submit their own written report to the contractor's security violation and any corrective actions taken by the contractor and the AR to resolve the security issues.
    - The contract is subject to termination by the AR for any security violations related to CHRI if the contractor fails to notify the AR regarding such violations, or if the contractor refuses or is not capable of taking appropriate corrective action.

The Compact Council has the authority to suspend or terminate the authorized recipient's exchange of criminal history record information if the authorized recipient fails to notify the state compact officer of any security violations, or refuses to or is not capable of taking corrective action in resolving the security violations. If criminal history record information has been suspended, it may be reinstated pending written verification from the authorized recipient, the contractor, and the state compact officer to the Compact Council or the United States attorney general that the security violation has been successfully resolved. If access to criminal history record information has been terminated with the authorized recipient, then the contractor's records containing criminal history record information must be deleted or returned with the appropriate time frame as specified by the authorized recipient.

In view of the stringent requirements for security and concern for any unauthorized access to criminal history record information, the authorized recipient must be assured that the contractor is capable of adhering to all technical and procedural security requirements per the FBI CJIS Security Policy before outsourcing any functions requiring access to criminal history record information to a contractor.

7.5 EXEMPTIONS

It has become more common to allow documents to be maintained electronically and/or hard copies to be stored or archived off-site by third-party contractors. While an outsourcing contract is required in these circumstances, there may be sections of the Outsourcing Standard that may be omitted from the contract when specific conditions apply.

7.5.1 Exemption 1: IT Contractor. When an authorized recipient contracts with an IT contractor, the outsourcing contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0 and 9.0 of the Outsourcing Standard for non-Channelers when **all** of the following conditions exist:

1. Access to criminal history record information by the IT contractor's personnel is limited solely for the development and/or maintenance of the authorized recipient's computer system;
2. Access to criminal history record information is incidental, but necessary, to the duties being performed by the IT contractor;
3. The computer system resides within the authorized recipient's facility;
4. The authorized recipient's personnel supervise or work directly with the IT contractor personnel;
5. The authorized recipient maintains complete, positive control of the IT contractor's access to the computer system and criminal history record information contained therein; and
6. The authorized recipient retains all of the duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard.

If all the above conditions exist, there are areas of the Outsourcing Standard that do not apply to the IT contractor. Some of the requirements pertain to the authorized recipient's knowledge of the contractor's technical system specifications. If applicable, the authorized recipient will not be required to understand the contractor's communication and record capabilities, and will not be required to maintain topological drawings of the network configuration. The contractor will not be subject to audit by the authorized recipient within the first 90 days, nor will the authorized recipient be required to notify of any early termination of the contract to the compact officer. The contractor will not be required to implement a Security Program or security training for employees that have access to criminal history record information and contractor's facilities will not be subject to audits. Other areas, such as criminal history record information retention policies and some dissemination policies will not be applicable, as criminal history record information is not being used by the contractor for any noncriminal justice function other than its incidental access for IT purposes

7.5.2 Exemption 2: Storage/Retrieval/Destruction Contractor. When an authorized recipient contracts for storage, retrieval, or destruction, the outsourcing contract need only include Sections 1.0, 2.01, 2.03, 3.01, 4.0, 6.0, 8.0 and 9.0 of the Outsourcing Standard for Non-Channelers when **all** of the following conditions exist:

1. Access to criminal history record information by the government contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the criminal history

record information at the government contractor's facility; (B) retrieval of the criminal history record information by government contractor personnel on behalf of the authorized recipient with appropriate security measures in place to protect the criminal history record information; and/or (C) destruction of the CHRI by government contractor personnel when not observed by the authorized recipient.

2. Access to criminal history record information is incidental, but necessary, to the duties being performed by the government contractor.
3. The government contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the authorized recipient.
4. The government contractor's personnel are subject to the same criminal history record checks as the authorized recipient personnel.
5. The criminal history record checks of the government contractor personnel are completed prior to work on the contract or agreement.
6. The authorized recipient retains all other duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard.
7. The government contractor stores the criminal history record information in a physically secure location.

When an authorized recipient contracts for storage, archiving, retrieval, and/or destruction, the contract may exclude portions of the Outsourcing Standard provided all the above conditions are met. Areas concerning the contractor's technical system and networking configuration will not need to be known to the authorized recipient. The contractor will not be required to implement a Security Program or Security Training Program and will not be subject to a mandatory facility or Security Program audit.

The difference between the two exemptions stated above is that in addition to Sections 1.0, 2.01, 2.03, 3.01, 6.0, 8.0 and 9.0 of the Outsourcing Standard, the contract for storage, retrieval, and/or destruction must also include Section 4.0. Section 4.0 requires the contractor to maintain site security ensuring that criminal history record information is stored in a physically secure location and protected against any unauthorized access.

7.6 Steps For Implementing An Outsourcing Contract

When an agency wants to outsource a noncriminal justice administrative function that requires a third-party contractor to have access to criminal history record information, the following steps should be followed:

1. Contact the MSHP-CJISD and ask for your regional auditor/trainer. (See Appendix A)
2. Obtain the most current version of the Security and Management Control Outsourcing Standard (SHP-570).
3. Draft the contract between the agency or authorized recipient and the contractor. Your agency will be provided with sample contract wording to be used as a guideline. Sample contract wording is also shown below.

4. Prior to finalizing a contract with a third-party, it is recommended that the proposed contract wording be sent to the MSHP-CJISD for review.
5. Submit a formal letter of request and a copy of the contract to the MSHP-CJISD for review.

As a reminder, prior to the outsourcing approval, disclosure of criminal history record information to an outside entity or third party contractor is strictly prohibited and may be deemed misuse. (See Section 4, Dissemination)

7.7 Sample Contract Wording

Below is sample contract wording that must be incorporated in your agency contract with the third party/contractor:

This contract is entered into between [insert authorized recipient's name and address], the authorized recipient, and [insert contractor's name and address], the contractor, under the terms of which the authorized recipient is outsourcing the performance of noncriminal justice administrative functions involving the handling of criminal history record information pursuant to Title 28, Code of Federal Regulations, Part 906 and the relevant Security and Management Control Outsourcing Standard for Non-Channelers (Outsourcing Standard), and the relevant CJIS Security Policy. The most current version of the Outsourcing Standard and CJIS Security Policy are incorporated by reference into this contract and appended hereto as Attachments [insert attachment #].

The authorized recipient's authority to submit fingerprints for noncriminal justice purposes and to obtain the results of the fingerprint search, which may contain CHRI, is [insert the legal citation of the state statute]. This authority requires or authorizes fingerprint-based background checks of [insert all categories of current and prospective employees, licensees, or applicants for other benefits covered by state statute].

The specific noncriminal justice administrative function(s) to be performed by the contractor that involve access to CHRI on behalf of the authorized recipient is to [insert specific noncriminal justice administrative functions to be performed, e.g., obtaining missing dispositions, making fitness determinations and/or recommendations, storing of or destruction of criminal history record check results].

[Insert contractor's name] will comply with the Outsourcing Standard requirements, CJIS Security Policy, and other legal authorities to ensure adequate privacy and security of personally identifiable information and criminal history record check results related to this contract, and will ensure that all such data is returned to the authorized recipient when no longer needed for the performance of contractual duties.

A copy of the signature page with dates must be included with the contract.

SECTION 8: FINGERPRINT SUBMISSION

8.1 Fingerprint Submission To The MSHP-CJIS

There are three options for fingerprint submission to the MSHP-CJIS:

1. Electronic Fingerprint Submission — MACHS Website
2. Manual Fingerprint Submission Using The Applicant Fingerprint Card (FD-258)
3. The Patrol's Public Window For Electronic Submission — General Headquarters Annex Building

Several agencies require specific fingerprint submissions. For instance, they may require that applicants use the Patrol's MACHS website for fingerprint registration and electronic fingerprint capture through the state electronic vendor. (See Option 1 below.) Applicants should refer to their agency for specific fingerprint instructions.

8.1.1 OPTION 1: MACHS Website For Registration. The Missouri Automated Criminal History Site (MACHS) is a system administered by the MSHP-CJISD. Each entity that has an approved ORI is assigned a four-digit MACHS registration number to use for registration process and electronic submission of fingerprints. The MACHS number is specific to the agency ORI and ensures that the criminal history record responses are disseminated to the authorized recipient.

Each agency is responsible to provide the MACHS registration number to their applicants prior to fingerprinting. Agencies must ensure that their applicants understand the proper use of the MACHS registration number. Using a wrong number will result in the state and FBI responses being sent to another agency. The MACHS website has several safeguards in place that prompts the applicant to verify the information entered. However, if the information is not verified and results are not sent to the correct agency, the applicant may be required to begin the process over and may incur additional fees.

MACHS Website: www.machs.mo.gov

Enter the agency four-digit registration number (or MACHS number) in the box and click "enter." Follow the prompts for registration. At the conclusion of registration, a confirmation or transaction control number will be assigned. The applicant must take the transaction control number to the fingerprint location for fingerprinting.

While the electronic fingerprint vendor sites are required to verify the personal identifying information and capture fingerprint images on applicants for transmission to the MSHP-CJISD, they do not have access to criminal history record information. Any questions regarding background check results must be referred to the MSHP-CJISD. For assistance with questions, please contact MSHP-CJISD. (See Contact Information, Appendix A.)

8.1.2 OPTION 2: Manual Fingerprint Submission — Using FD-258 Applicant Fingerprint Card. County sheriff departments, local police departments and MSHP troop locations throughout Missouri may assist the public with fingerprint needs. Although several law enforcement agencies have access to a livescan (electronic) fingerprint device, law enforcement is not allowed to transmit applicant fingerprints to the MSHP-CJISD for civil background checks. Law enforcement must print the completed fingerprint card to give to the applicant for submission to the MSHP-CJISD. (Exceptions include CCW permits, city or county governments, and housing authorities.)

The FD-258 fingerprint card is a standardized FBI-issued card and is generally available at any law enforcement agency in Missouri and other states. When sending manual fingerprint cards to the Patrol for processing, they should be sent to:

MSHP-CJISD Annex Building
PO Box 9500
Jefferson City, MO 65102-9500

8.1.3 OPTION 3: MSHP-CJISD Public Window. The MSHP-CJISD Public Window is located at the MSHP's General Headquarters Annex Building at 1510 East Elm Street in Jefferson City, Missouri. Public window services are available Monday through Friday from 8 a.m. until 5 p.m. with the exception of state and federal holidays. Individuals needing a fingerprint-based background check may appear in person for electronic and ink fingerprint needs.

8.1.4 Out-Of-State Applicants — Whether the applicant is in Missouri or located out-of-state, manual fingerprint submission on a standard FD-258 Applicant Fingerprint Card can be utilized. The FD-258 Applicant Fingerprint Card is an FBI-issued card, and therefore, all law enforcement agencies should have the cards or an agency may request them from the MSHP-CJISD.

Agency options for out-of-state applicants are:

1. The agency may advise the applicant to go to their local law enforcement agency in their state and request to be fingerprinted on an Applicant Fingerprint Card (FD-258).
2. The agency can send a fingerprint card to the applicant and advise them to take the card to their local law enforcement agency to be fingerprinted.

Fingerprint card submission options include:

1. The completed Applicant Fingerprint Card can be mailed directly to the MSHP-CJISD for processing. Appropriate fees must accompany the fingerprint card unless the agency has established billing procedures. It is recommended that the applicant return the completed fingerprint card to the agency for verification of personal identifying information and to ensure the card is completed correctly (with the agency ORI, OCA, if applicable, and reason fingerprinted) to ensure proper processing.
2. The completed Applicant Fingerprint Card (FD-258) may be mailed to 3M Cogent, the Missouri contracted fingerprint vendor, for electronic submission to the MSHP-CJISD, which may expedite the processing time. Applicants are required to register on MACHS and obtain a transaction

control number (TCN). The TCN must be written on the back on the fingerprint card prior to mailing. For assistance, applicants may contact 3M Cogent at (877) 862-2425.

The state contracted vendor, 3M Cogent, does not process criminal history, nor do they have any access to criminal history or criminal history files. All processing of background checks for the state of Missouri and FBI are through the MSHP-CJISD.

8.2 Fingerprint Fees

The MSHP-CJISD does not charge for fingerprinting. The only fees charged are those associated with the background check. Fees are payable at the time of service unless the fees are being paid by an agency that has established a billing account. Payment in check or money order should be made payable to the Criminal Record System Fund. Credit and debit cards are also acceptable.

All fees for criminal history record information provided by the MSHP-CJISD and FBI are in accordance with Section 43.530 RSMo. and Title 28 Code of Federal Regulations 20.31(e)(3).

8.3 Fingerprint Submission, Chain Of Custody (Best Practice)

The National Crime Prevention and Privacy Compact Council (Compact Council) is a 15-member body of local, state, and federal governmental officials, which prescribes system rules and procedures for the effective and proper operation of the III for noncriminal justice purposes. The demand for fingerprint-based background checks for noncriminal justice purposes has increased. Fingerprinting agencies and contractors alike have expressed concern that applicants with a criminal history record may have someone pose as the applicant for fingerprinting purposes. Based on the Compact Council's Best Business Practice, it is recommended to request and obtain photographic identification when capturing an individual's fingerprints. Do not provide the fingerprint card to the applicant to submit, as the applicant could alter the card.

8.3.1 Primary & Secondary Identification — Most agencies request some type of photo identification card as one method for verifying an individual's identity. The Compact Council suggests agencies accept only current, valid, and unexpired picture identification documents. As a primary form of picture identification, an applicant may present a state-issued driver's license, which meets the requirements of Public Law 109-13 when being fingerprinted. However, in the absence of the driver's license, applicant may provide one or more secondary documents including:

- State Identification Card (if the state's identification card standards are the same as the driver's license);
- State Government Issued Certificate Of Birth;
- U.S. Active Duty/Retiree/Reservist Military Identification Card;
- U.S. Passport;
- Federal Government Personal Identity Verification Card;
- Department Of Defense Common Access Card;
- U.S. Tribal Or Bureau Of Indian Affairs Identification Card;
- Social Security Card;

- Court Order For Name Change/Gender Change/Adoption/Divorce;
- Marriage Certificate (Governmental Certificate Issued);
- U.S. Government Issued Consular Report Of Birth Aboard;
- Foreign Passport With Appropriate Immigration Documents;
- Certificate Of Citizenship;
- Certificate Of Naturalization;
- INS Resident Alien Card (issued since 1997);
- ISN Temporary Resident Identification Card; or,
- ISN Employment Authorization Card.

When validating the authenticity of secondary identification documents and forms, the data and information may be supported by at least two of the following:

- Utility bill (showing address);
- Jurisdictional Voter Registration Card;
- Vehicle Registration Card/Title;
- Paycheck stub with name and address;
- Jurisdictional Public Assistance Card;
- Spouse/Parent affidavit;
- Canceled check or bank statement, or,
- Mortgage documents.

When an agency has a reason to believe an applicant has presented fraudulent information, agency personnel should contact local law enforcement. No attempt should be made to detain or pursue the person.

An agency may employ a process to protect the integrity of the applicant's fingerprints when they are forwarded to the state's central repository. Some examples include: Establish provisions for the agency to manage both manually and electronically captured fingerprints; establish an agency tracking system (applicant log) using the employee's name or some other method for identifying the individual capturing the fingerprints and verifying the applicant's identity; establish procedure that documents the type of identification used by the applicant; establish procedures that use specially sealed envelopes, agency specific stamps, etc., for the agency to use when forwarding the applicant's manual fingerprint card; and implement the use of forms.

8.4 First Rejection & Second Submission Procedures

There are several reasons that cause an applicant's fingerprints to be rejected by the MSHP-CJISD or FBI. Some of these reasons consist of:

1. The quality of characteristics is too low.

2. Fingerprint images are incomplete, out of sequence.
3. Fingerprint patterns are not discernable.
4. Reason fingerprinted is incorrect or has no statutory authority.

In any of these instances, a second fingerprint submission is required to receive the full criminal history record requested. A second submission is free of charge as long as it is submitted timely.

8.4.1 First Rejection — Manual Submission. If a fingerprint is submitted manually and is rejected by the MSHP-CJISD or the FBI, a letter will be sent back to the address of the applicant or agency with instructions on how to submit a second set of fingerprints. There is no cost for the second submission if completed during a timely manner. An ECN number will be included on the return instructions.

8.4.2 First Rejection — Electronic Submission Through MACHS/Vendor. When a fingerprint is rejected from electronic submission, a notice will be provided to the applicant by the fingerprint vendor. The notice will include instructions on how to proceed with the second fingerprint submission, as well as the ECN number. There is no cost for a second submission when the second submission is completed in a timely manner.

8.4.3 Second Rejection — FBI Name Check Procedure. When fingerprint images are rejected a second time (by the FBI), an agency has the option to request a name check through the FBI. The agency will receive paperwork to be faxed to the FBI to request the name search. The name check result will be sent directly from the FBI to the agency, with the exception of VECHS agencies. (The MSHP-CJISD is the authorized recipient for VECHS ORIs and thus the FBI will only respond to the MSHP-CJISD. The MSHP-CJISD, in turn, will send the results to the VECHS agency.) As a reminder, since the name-based search is not fingerprint-based, the results are not guaranteed.

8.5 Challenge Procedures

The applicant may contact the Missouri State Highway Patrol Applicant Section for obtaining information on how to challenge, correct, or update the Missouri criminal history record.
If the applicant is challenging the accuracy or completeness of the FBI criminal history record, they should send the challenge to the agency that contributed the questioned information or they may send a challenge directly to the FBI. The FBI will then forward their challenge to the agency that contributed the questioned information and request the agency to verify or correct the challenged entry.

8.6 Applicant Procedures For Obtaining Personal Record

8.6.1 From MSHP-CJISD — Any person/applicant may obtain a state (Missouri) background check on themselves through the MSHP-CJISD. The applicant has three options:

1. Go to the MACHS website (www.machs.mo.gov) and conduct a name-based search or register for a fingerprint background check. To obtain the four-digit registration number for a personal review based on fingerprints, the applicant must contact the MSHP-CJISD at (573) 526-6153, or
2. Come to the Patrol's Annex Building Public Window, located at 1510 E. Elm Street in Jefferson City, to be fingerprinted, or
3. Mail a manual fingerprint card (FD-258) with payment to the MSHP-CJISD.

8.6.2 From The FBI — If an applicant desires a background check from the FBI, they will be required to complete an Applicant Fingerprint Card (FD-258) and mail it directly to the FBI. Fees and instructions for submitting a fingerprint card to the FBI are available on the FBI's website (shown below). The applicant may contact their local law enforcement or the MSHP-CJISD for fingerprinting assistance.

http://www.fbi.gov/about-us/cjis/criminal-history-summary-checks/submitting-a-criminal-history-summary-request-to-the-fbi

SECTION 9: CRIMINAL HISTORY

9.1 Generating A Criminal History

Criminal history record information is submitted to the MSHP-CJISD by means of the charge information contained on the criminal fingerprint card or criminal livescan submission by law enforcement and is tracked by means of the Offense Cycle Number (OCN). After fingerprints have been entered and identified through the Automated Fingerprint Identification System (AFIS) and matched to or assigned a State Identification Number (SID), the arrest is entered into criminal history for the individual. Thus, making the fingerprint submission is the most critical element when creating a criminal history record. It is especially important due to criminals providing alias information or committing identity theft. Without the fingerprint submission, criminal history will not be present.

9.1.1 The OCN — Offense Cycle Number indicates an arrest and is also referred to as the tracking number of the arrest. Each OCN in a criminal history record represents an arrest. When an individual is arrested and fingerprinted, the OCN is generated from the fingerprint card and is entered into criminal history after the prints are identified through AFIS (Automated Fingerprint Identification System). When a Record of Arrest and Prosecution (RAP) sheet is requested on an individual that has criminal history, each OCN listed on the RAP sheet will indicate a separate arrest. There may be one or more charges present with each OCN. The OCN is crucial to prosecutors and courts when submitting prosecutor action and court disposition to the Central Repository.

9.1.2 The SID — State Identification Number is assigned to the first set of fingerprints received on an individual at the Central Repository. A SID number does not indicate that a person has a criminal record. Every person fingerprinted in Missouri, whether for civil purposes, such as employment or licensing, or from a criminal arrest card stemming from an arrest by law enforcement, will have an assigned SID once the fingerprints are processed through AFIS. This SID number for Missouri will accompany the individual throughout their life and will never change.

9.1.3 The *Missouri Charge Code* is the state statute that describes the crime and associated penalties used by criminal justice agencies. The charge code will indicate felony, misdemeanor, infractions, and local ordinance charges and classifies each offense according to the law.

Contributing agencies include law enforcement agencies, prosecutors, courts, Department of Mental Health, and Department of Corrections.

Criminal history record information is defined and has three parts as follows:

- The arresting agency's name and crime class under which the person was arrested. The arrest data submitted includes the mandatory field of name, race, sex, and date of birth. All arrests are accompanied by fingerprints.
- The charge(s) issued by the prosecutor.

- The name of the court that tried the case and the ultimate disposition of the case.

Criminal history record information and custody information is compiled from information submitted to the MSHP-CJISD from contributing agencies. Although the MSHP-CJISD makes reasonable efforts to ensure all information is submitted as required by law, it is not responsible for omissions from contributing agencies.

Criminal history record information is constantly being updated as new arrests and other information are entered into the system by contributing agencies. Certain statutes allow for the suppression or deletion of records, such as expungements, and when this occurs, this information is not retained in the system. (See Sections 610.120, 610.123 and 610.140 RSMo. for arrest expungement information and Section 577.054 RSMo. for alcohol-related expungements.)

9.1.4 Criminal History Records — Missouri records based on fingerprint submission and legislative authority include all criminal history data contained within the systems of the MSHP-CJISD. The data includes all arrests, filed and not filed charges, charges that have been nolle prossed, dismissed charges, or a found not guilty in a court of law determination, and will include any suspended imposition of sentence (SIS) during and after the probationary period.

Open records include convictions and plea of guilt, arrest charges within the first 30 days, pending charges, and suspended imposition of sentence (SIS) while on probation.

Closed records includes all open records in addition to those accused and found not guilty, charges that were nolle prossed or dismissed, an SIS after probation is complete, and arrests after 30 days when no charges have been filed.

FBI criminal history obtained through the MSHP-CJISD contains arrest data from all contributing states. Records include those retained within the systems of the FBI and those held by NFF states.

Once fingerprints and arrest information are received at the MSHP, the record information is always retained with the exception of expungement.

9.2 Record Of Arrest & Prosecution (RAP) Sheet

A RAP sheet is a listing of certain information taken from fingerprint submissions retained by the MSHP-CJISD and the FBI. If the fingerprints are related to an arrest, the RAP sheet will include the name of the agency that submitted the fingerprints to MSHP-CJIS or the FBI, the date of the arrest, the arrest charge, and the disposition of the arrest, if known. All arrest data included in a RAP sheet is obtained from fingerprint submissions, disposition reports, and other information submitted by agencies having criminal justice responsibilities.

A RAP sheet may be generated when fingerprint submissions are received by the MSHP and FBI. Applicant fingerprint submissions by agencies having authority to receive full criminal history record information will receive Missouri open and closed information, as well as, any records maintained by the FBI.

When a RAP sheet is requested for an individual that has criminal history, each OCN listed on the RAP sheet will indicate a separate arrest. There may be one or more charges present with each OCN. A RAP sheet is considered complete when you have the arrest, prosecution, and court information. Other agencies that submit information to the criminal history record repository will be listed as part of the disposition. Non-criminal justice agencies use background checks for employment, licensing, adoption, citizenship verification, and firearm purchases. In any of these cases, if a disposition is not present on the applicant's record, this could prevent or delay finalization of these proceedings.

9.3 Expungement Of Arrest Records

The procedures for an individual to file a petition to expunge an arrest record are contained in Section 610.123 RSMo. The statute states, in part, that any person who wishes to have a record of arrest expunged pursuant to Section 610.122 RSMo. may file a verified petition for expungement in the civil division of the circuit court in the county of the arrest. Individuals seeking to have an arrest, plea, trial, or conviction expunged should contact the circuit court in the county where the arrest occurred and file a petition for "Expungement of Arrest Record." (Missouri Court Criminal Form, CR 145, Petition for Expungement of Arrest Records. This form is used to ask the court to order agencies that have arrest records pertaining to a specific incident in which the applicant was involved to destroy those records. All agencies that may have records must be identified by checking the appropriate boxes. For more information, refer to court website, www.courts.mo.gov/file.jsp?id=647)

9.3.1 The petition must specifically identify the Central Repository. For an arrest record to be removed from the MSHP's system, the petition must include the Central Repository. If a petitioner does not include the Central Repository, any information housed within the criminal history record system will not be removed. The Central Repository is only authorized to expunge a record upon receipt of a court order naming the Central Repository as a defendant. When an order to expunge is received, the Central Repository will make a request to the FBI to expunge the record if the record to be expunged is contained also within the FBI system.

9.3.2 Fingerprints are required. An individual filing for a petition to expunge must also provide the court with a complete set of their fingerprints on a standard fingerprint card which will be forwarded to the Central Repository and used for the purpose of positively identifying the petitioner.

9.3.3 Specific conditions must be met. Notwithstanding other provisions of law to the contrary, any record of arrest recorded pursuant to Section 43.503 RSMo. may be expunged if the court determines that the arrest was based on false information and the following conditions exist:

1. There is no probable cause at the time of the action to expunge to believe the individual committed the offense.
2. No charges will be pursued as a result of the arrest.
3. The subject of the arrest has no prior or subsequent misdemeanor or felony convictions.
4. The subject of the arrest did not receive a suspended imposition of sentence (SIS) for the offense for which the arrest was made or for any offense related to the arrest.
5. No civil action is pending relating to the arrestor the records sought to be expunged.

Certain offenses may also be expunged when there was a finding of guilt, plea, trial, or conviction (Section 610.140 RSMo.). Offenses that may qualify for expungement include:

1. Any felony or misdemeanor offense of passing a bad check under Section 570.120 RSMo., fraudulently stopping payment of an instrument under Section 570.125 RSMo., or fraudulent use of a credit device or debit device under Section 570.130 RSMo.
2. Any misdemeanor offenses pursuant to Sections 569.065, 569.067, 569.090, subdivision (1) of Subsection 1 of Section 569.120, Sections 569.140, 569.145. 572.020, 574,020, or 574.075 RSMo.
3. Any class B or class C misdemeanor offense pursuant to Section 574.010 RSMo.

9.3.4 After a petition is filed with the court, the court will set a hearing date no sooner than 30 days from the filing date of the petition. When named in the petition, a Notice of Hearing, along with the petition to expunge and a copy of the petitioner's fingerprints, are forwarded to the Central Repository. The MSHP-CJISD will review any records contained within the Central Repository and will make a recommendation to the MSHP's Custodian of Records on whether or not to contest the petition.

9.4 National Fingerprint File (NFF)

9.4.1 National Fingerprint File (NFF) States — There are 18 current NFF state participants. In 2013, Missouri became the 17th state to be approved for NFF participation by the FBI CJIS Division. For a list of NFF states, please refer to the FBI's website at www.fbi.gov.

9.4.2 Benefits Of Record Control — NFF states control record usage. An NFF participating state is queried directly for its record via III. The III record request identifies the purpose for the request, providing the NFF state the benefit of always knowing when its records are being used and for what purpose.

An NFF state provides its records for all purposes; thus, any request for an NFF state's maintained record when a national fingerprint-based check is conducted, results in the NFF state's repository being queried directly for its CHRI.

An advantage to being an NFF state is the reduction of duplicative record maintenance. Once the decentralization occurs and the NFF state fully maintains their criminal history records, there is no need to duplicate records at the federal level. Missouri is not required to forward expungement notices and disposition information to the FBI. Once a record is initially indexed at the FBI, subsequent arrest submissions are not required.

SECTION 10: STATE AGENCY, BOARD, OR COMMISSION

10.1 Access & Use — Based On Public Law 92-544 & State Statute

Pursuant to Public Law 92-544, the FBI may exchange CHRI with officials of state and local governments for purposes of licensing and employment if authorized by a state statute. The purpose and use of the CHRI must be specifically stated in state statute, and must indicate that the request is fingerprint-based and includes access to national criminal history. The legislative authorization must, expressly or by implication, authorize the use of the FBI records for screening the applicant.

Most state agencies qualify for access to fingerprint-based CHRI through Revised Statutes of Missouri. Some state agencies have agency-specific laws, i.e. Missouri Gaming Commission, Department of Social Services, Department of Health and Senior Services, Missouri Public School Districts, and Missouri Lottery Commission. In addition, the Missouri Board of Professional Registration oversees 38 professional boards which many require a state and FBI background check be conducted prior to licensure. The statutes that are relative to their agency are specific to what they can request and obtain based on a specific purpose.

There are numerous state agencies in Missouri with ORIs. In order to receive an ORI, the agency would have requested an ORI and provided the authorizing state statute. Some agencies have access to CHRI and do not request CHRI. Others have access but only request a state background check, while others request both a state and FBI background check. It is ultimately the state agency's decision whether to request criminal history and from which systems, i.e. the state or both state and FBI.

10.2 Requesting Access

If a state agency does not have an ORI and wishes to obtain an ORI, the agency representative should contact the MSHP-CJISD to begin the process.

If a new ORI is needed or if the agency previously had an ORI and the ORI is no longer active, the MSHP-CJISD auditor/trainer can assist the agency in drafting the appropriate request letter.

Information to be included in the letter is as follows:

- The specific information about the category of applicants, i.e. employees, prospective employees, volunteers;
- The purpose of the screenings;
- The statute that authorizes the receipt of CHRI;
- The state agency Point of Contact (POC) information; and
- If an ORI was previously assigned and now retired, include the ORI number, if known.

Once received, the MSHP-CJISD will make a formal written request to the FBI for ORI approval.

When the approval notification is received from the FBI, the MSHP-CJISD will establish a point of contact with the state agency. The POC will usually be the person designated to receive and maintain the criminal history record information for the state agency and will also be the contact person when scheduling the Policy Compliance Reviews. Upon ORI approval, the agency will be added to the audit cycle and the regional CJIS Auditor/Trainer will provide the agency POC with appropriate documentation to assist the agency with the PCR process.

It is important for good communication to be established between the POC of the agency and the MSHP-CJISD. For any clarifications needed regarding the use of criminal history, or if any questions arise regarding an applicant's criminal history report, record challenge or dissemination procedures, the POC is encouraged to contact the regional auditor/trainer for assistance.

SECTION 11: VECHS AGENCIES

11.1 ACCESS TO CHRI — BASED ON FEDERAL LEGISLATION & MISSOURI VECHS PROGRAM PROCEDURES

In 2006, the FBI notified the MSHP-CJISD that the dissemination of an individual's criminal history record information to a nongovernmental entity with the individual's consent and at his/her direction is not legally objectionable under federal law. (See FBI CJIS Information Letter dated Nov. 2, 2006.)

The safety and well-being of children and other vulnerable individuals is a national priority. The National Child Protection Act, as amended by the Volunteers for Children Act, encourages states to authorize fingerprint-based national criminal history record information background checks of individuals having access to children and other vulnerable people, by enacting legislation under Public Law (Pub.L.) 92-544. The NCPA/VCA also authorizes entities in states without specific Pub. L. 92-544 legislation to obtain national criminal history record information checks. (Title 42 U.S.C. Section 5119a)

The success of this national initiative of child protection is dependent on the cooperation by the states in the implementation of the NCPA/VCA and other federal or state legislation. (Refer to Prosecutorial Remedies and Other Tools to End the Exploitation of Children Total Act of 2003 and the Adam Walsh Child Protection and Safety Act of 2006, Public Law 109-248.) Many states have established programs for conducting criminal history record background checks on individuals who work with children, the elderly, or the disabled. Prior to the MSHP-CJISD establishing the Missouri VECHS (Volunteer and Employee Criminal History Service) program, a VECHS program was developed by the Florida Department of Law Enforcement. Florida's VECHS program used the basic framework of the NCPA/VCA with the added feature of dissemination of an individual's criminal history record to nongovernmental entities at the applicant's request. By establishing strict controls on the access and use of criminal history record information by entities enrolled in the VECHS program, the Florida Department of Law Enforcement had created a program that facilitates the performance of criminal history record checks on thousands of individuals who work with children, the elderly, and individuals with disabilities.

As a result of the success of the Florida VECHS program, the Compact requested the FBI to provide advice on the dissemination under the NCPA/VCA of an individual's CHRI to a nongovernmental entity with the individual's consent. The FBI has no legal objection to the dissemination of CHRI at the consent of the individual, as the practice does not conflict with federal law. (Title 5 USC 552a (d) (1) and (t) (1).) The FBI advised that other states planning to establish CHRI background check programs, that include the dissemination of CHRI to NGEs, must incorporate the following provisions:

- The state shall establish procedures for program participation by nongovernmental entities which serve children, elderly, or individuals with disabilities.
- The nongovernmental entities must execute a user agreement that sets out the terms under which the criminal history record checks may be performed. This includes the security requirements for protection of the CHRI and the procedures for challenging the accuracy and

completeness of the CHRI as entitled by the NCPA/VCA and 28 Code of Federal Regulation 50.12.

- The nongovernmental entity shall obtain an executed consent form (waiver) from every employee or volunteer subjected to the criminal history record check. The nongovernmental entity shall retain the original waiver and transmit a copy to the state. (In lieu of transmitting the waiver to the state, the MSHP-CJISD verifies waivers during the audit process.) The terms of the waiver must include an acknowledgement that the entity will perform an FBI criminal history records check and that the state is specifically authorized to disseminate the resulting CHRI, if any, to the nongovernmental entity. The waiver may further authorize the nongovernmental entity to provide the CHRI to another nongovernmental entity. The nongovernmental entity must maintain a record of any secondary dissemination.

The MSHP's VECHS program was developed in 2008 to provide agencies or "qualified entities" that provide care or care placement services to children, the elderly, or individuals with disabilities access to Missouri open and closed criminal history records and FBI criminal history record information with fingerprint submission.

11.1.1 The term "care" means the provision of care, treatment, education, training, instruction, supervision, or recreation to children, the elderly, or individuals with disabilities. (Section 43.540 RSMo. and NCPA/VCA)

11.1.2 The term "qualified entity" means a business or organization, whether public, private, for-profit, not-for-profit, or voluntary, that provides care or care placement services, including a business or organization that licenses or certifies others to provide care or care placement services.

11.1.3 The term "provider" means a person who is employed by or volunteers with a qualified entity; owns or operates a qualified entity; or who has or may have unsupervised access to a person to whom the qualified entity provides care; and a person who seeks to be employed by or volunteer with a qualified entity; seeks to own or operate a qualified entity; or seeks to have or may have unsupervised access to a person to whom the qualified entity provides care.

11.1.4 The term "person" refers to child, elderly, or individuals with disabilities.

The qualified entity may choose to deny the provider unsupervised access to a person to whom the qualified entity provides care.

The VECHS program requires the completion of an application and user agreement. The Missouri VECHS program is authorized pursuant to these federal acts:

- The National Child Protection Act, as amended by Volunteers for Children Act (NCPA/VCA); and
- The Adam Walsh Child Protection Act (Adam Walsh Act), Section 153 Schools Safe Act (Schools Safely Acquiring Faculty Excellence Act of 2006).

11.1.5 ORIs For VECHS. As the authorized recipient for criminal history record information obtained through the VECHS program, the MSHP-CJISD allows VECHS approved agencies to use the ORIs for requesting criminal history record information. Dissemination from the MSHP to VECHS agencies is authorized through the use of the waiver form and user agreement. Each ORI is specific to the federal legislation as shown below:

- MOVECHS0Z (NCPA/VCA)
- MOAWA000Z (Adam Walsh Act)

Program approval is based on the specific federal act that applies to the agency. Although the primary legislation for the VECHS program is the NCPA/VCA, private elementary and secondary schools wanting to background check employees would qualify under the Adam Walsh Act Section 153; agencies that are mandated to conduct background checks on employees or volunteers pursuant to the Edward M. Kennedy Serve America Act would qualify under NCPA/VCA. (Title 42 USC Section 12645g, as referenced in Section 189D (Public Law 111-13)

Since the VECHS program is not based on Missouri statute (Public Law 92-544), all VECHS agencies are required to use a Waiver Agreement and Statement. The Waiver Agreement and Statement adheres to the FBI requirement of Title 28, 16.30-34 and is auditable. Each agency must provide the waiver to the applicant **prior** to requesting them to be fingerprinted. The waiver gives the agency permission from the applicant to obtain their FBI criminal history record, if any, from the MSHP-CJISD. Each VECHS entity is required to produce the waivers during the audit review. Failure to produce waivers during audit will result in a noncompliance assessment and may require a follow up audit.

With agency approval, the MSHP-CJISD allows the agency to use an ORI with an assigned OCA for fingerprint submission and receipt of state and FBI criminal history records. The OCA number is a unique nine-digit number assigned to each agency and identifies the agency by county. Because there are multiple agencies enrolled in VECHS and using the same ORIs, the OCA number is required for tracking and dissemination purposes. All dissemination of criminal history records from the MSHP-CJISD to the VECHS agency is tracked by the ORI and OCA and is used for auditing purposes.

In addition to the assigned ORI and OCA, each agency is also assigned a four-digit MACHS number to use for electronic fingerprint submission, if they choose to submit via the electronic method. Both ink fingerprint cards and electronic submission are acceptable. For ink submission, the approval packet will include a small amount of Applicant Fingerprint Cards (FD-258) that are pre-printed with the ORI for agency use. (See Section 8 Fingerprint Submission Procedures)

11.2 Steps To Apply For VECHS Enrollment

11.2.1 VECHS Enrollment:

1. Does your agency, school, or business provide care to children, the elderly, or individuals with disabilities? If yes, continue.
2. Is your agency a lawful Missouri business, licensed, and with a physical operating address in Missouri? If yes, continue.
3. Complete a VECHS Application (SHP-980).
4. Complete a VECHS User Agreement (SHP-982).
5. Mail the completed application, user agreement, and your Missouri business license to the MSHP-CJISD, at P.O. Box 9500, Jefferson City, Missouri 65102-9500.

An electronic application and user agreement are available on the MSHP website.

The approval process will take appropriately two weeks. Upon verification of eligibility, the approval notification will be sent through email notification and through the mail with an approval packet containing program documents. Program packet approval documentation generally includes:

1. A copy of the completed application;
2. The signed user agreement between agency and MSHP-CJISD;
3. The Waiver Agreement and Statement (SHP-981);
4. A dissemination log sample;
5. MACHS fingerprint Instructions; and
6. Manual fingerprint cards (FD-258) (ink method) and instructions for manual submission.

For questions about the VECHS program or status of your VECHS application, contact MSHP-CJISD at 573-526-6153 and ask for the VECHS program. (See Appendix A)

Temporary employment agencies or job placement agencies that provide workforce personnel within agencies that serve children, the elderly, or individuals with disabilities are not eligible for enrollment in the VECHS program.

SECTION 12: Court Access To Criminal History — Civil Functions

12.1 Access & Use

Courts, like law enforcement agencies, have dual roles regarding access and use of criminal history records since they are a criminal justice entity and also a noncriminal justice entity when acting in the role of civil or noncriminal justice court functions. This section specifically addresses access to criminal history, with fingerprint submission, for purposes other than criminal justice administration.

For noncriminal justice access to criminal history, courts may apply for a noncriminal justice ORI. The noncriminal justice ORI will provide access to criminal history record information and may be used for eligibility or fitness determinations prior to granting access to minors, the incapacitated, the elderly, or individuals with disabilities. The authority for a court to request and obtain criminal history record information is pursuant to Sections 43.540, 210.160, and 453.070 RSMo. and includes the following category of persons:

- Prospective Adoptive Parents
- Guardian ad litems
- Conservators
- Court Appointed Special Advocates (CASA)
- Personal Representatives

With an ORI for noncriminal justice purposes, courts have the ability to request fingerprint-based criminal history record information from the state and FBI for the above purposes.

Although the court is a criminal justice agency and has access to criminal history record information relating to criminal justice functions, courts are not authorized to request or obtain criminal history record information from law enforcement agencies with direct terminal access through MULES/NCIC for noncriminal justice purposes. Law enforcement agencies are advised that if they receive a request from the court for criminal history record information for a noncriminal justice purpose as stated above, the court should be referred to the MSHP-CJISD for assistance with obtaining an ORI or instructions of proper use and access of criminal history record information.

SECTION 13: City/County Government — Access To CHRI

13.1 Authority & Use

Municipal and county government access to CHRI is authorized pursuant to Section 43.535 RSMo. By local or county ordinance, background checks based on fingerprints of applicants or licensees in specified occupations for the purpose of receiving criminal history record information is authorized by local or county officials.

Specific occupations or categories of persons must be in detail. For example:

- applicants applying for vehicles for hire,
- taxicab license,
- city or county employment,
- volunteers with the city/county government or parks and recreation governed by the city or county,
- security guards that are armed and unarmed,
- liquor licenses,
- solicitors, and
- peddler licenses, etc.

13.2 Procedure For Requesting CHRI

1. The city or county government must enact an ordinance that authorizes state and national fingerprint-based criminal history on applicants in specific occupations or categories of persons.
2. Once the ordinance has been approved, the city or county government will send a letter of request for an ORI and a copy of the approved ordinance to the MSHP-CJISD. (See Appendix E, Forms for sample letter.)
3. The MSHP-CJISD will review the documents.
4. The MSHP-CJISD will send a letter of request and the ordinance copy to the FBI for review and ORI approval.
5. The FBI will either approve or disapprove the ORI request and will notify the MSHP-CJISD.
6. If approved by the FBI, an ORI is assigned and approval notification is sent to the MSHP-CJISD.
7. The MSHP-CJISD notifies the city/county government and provides instructions for use.
8. The city or county government will need to decide what fingerprint method(s) they want to use. (See Section 8 — Fingerprint Submission.)

In addition to the fingerprint instructions outlined in Section 8, a city or county government may request their local law enforcement agency to assist with fingerprint submission. If the law enforcement agency has a livescan device and is willing to take the fingerprints and transmit to the MSHP-CJISD, the following is required:

1. The ORI must be added to the law enforcement agency livescan device. All transmissions must indicate the ORI for the city/county government.
2. An "Authorization To Invoice" must be completed by the city/county government. This form will enable the MSHP-CJISD to bill for the electronic fingerprint submissions.
3. For electronic fingerprint submission by a law enforcement agency, the agency must ensure the following:
    - The ORI assigned to the city/county government is used.
    - The reason fingerprinted field must indicate Section 43.535 RSMo.
    - The record type must be "X" (state and FBI fees apply).

13.3 Suggested Language – City/County Ordinance

[¶ Enter Ordinance Number]

This ordinance is enacted pursuant to Section 43.535 RSMo., to regulate the issuance of licenses for [*list occupations, i.e. liquor licenses, solicitors/peddlers, etc*.] within the [*enter name of city or county*] and/or employment with [*enter name of city or county government*].

An [*applicant, employee, prospective employee, or volunteer*] seeking to engage in [list occupation(s)] shall submit his/her fingerprints to the Missouri State Highway Patrol Criminal Justice Information Services Division, along with appropriate fees. The Missouri State Highway Patrol CJIS Division will compare the subject's fingerprints against its criminal file and, if necessary, submit the fingerprints to the Federal Bureau of Investigation for a comparison with national criminal history records. The results of the Federal Bureau of Investigation check will be returned to the Missouri State Highway Patrol CJIS Division, which will disseminate the state and national results to [*enter name of city or county government*].

The [enter name of city/county government] shall render a fitness determination based upon the results of the criminal background check. In rendering a fitness determination, the [*enter name of city/county government*] will decide whether the subject of record has been convicted of or is under pending indictment for (a) a crime which bears upon his/her ability or fitness to serve in that capacity; (b) any felony or a misdemeanor which involved force or threat of force, controlled substances, or was a sex-related offense; or (c) enumerated disqualifiers.

The subject of record may request and receive a copy of his/her criminal history record information from the [*enter name of city/county government*]. Should the subject of record seek to amend or correct his/her record, he/she must contact the Missouri State Highway Patrol CJIS Division for a Missouri state record pursuant to Section 43.535 RSMo., and the Federal Bureau of Investigation for records from other state jurisdictions maintained in its file pursuant to Title 28, CFR 16.30-34.

13.4 Sample Letter To Request An ORI

Address letter of request to:

Captain Larry W. Plunkett Jr.
Director, Criminal Justice Information Services Division
Missouri State Highway Patrol
1510 E. Elm Street
P. O. Box 9500
Jefferson City, MO 65102-9500

Dear Captain Plunkett:

The [enter name of city or county government] would like to formally request an Originating Agency Identifier for use in submitting applicant fingerprints for receipt of state and national criminal history record information pursuant to our Ordinance No. [enter Ordinance #].

It is our understanding with the passage of this ordinance we have met the Public Law 92-544 criteria and Section 43.535 RSMo., to conduct background checks on applicants and licensees in specific occupations including [list the occupations that are specified in the ordinance]. A copy of our ordinance is attached for your review.

Thank you for your assistance with this request. Should you have any questions or need additional information, please do not hesitate to contact me.

Sincerely,

Representative's Name

Submit a copy of the approved ordinance and Letter of Request to the MSHP-CJISD. When the MSHP-CJISD receives the ORI approval, notification will be forwarded to the city/county government, along with fingerprint instructions, billing instructions, and audit requirements.

For assistance with obtaining an ORI pursuant to Section 43.535 RSMo., please contact your local regional auditor/trainer. (Appendix A)

SECTION 14: DSS Children's Division

14.1 Emergency Child Placement (Section 210.482 RSMo.)

14.1.1 Background — The routine placement of children is a civil function (noncriminal justice function) and does not authorize the use of criminal history inquiries via direct terminal access of MULES/NCIC by criminal justice agencies with the exception of emergency placement or exigent circumstances.

In October 2000, the Compact authorized and established procedures for obtaining CHRI for the placement of children in emergency situations or when "exigent" circumstances arise. Generally, “exigent circumstances” refers to an emergency, a pressing necessity, or a set of circumstances requiring immediate attention or swift action. In August 2004, Missouri approved the statute allowing for these checks through state and federal databases such as the Missouri criminal history repository and the Interstate Identification Index.

The III may be obtained when an authorized state agency is considering the placement of a child with neighbors, friends, or relatives due to the immediate unavailability of a parent or legal guardian.

The Compact's interpretation of emergency and exigent circumstances during the emergency placement of children holds that there are two legal principles involved:

1. Exigent circumstances — when time is of the essence and the health and safety of the child are involved, and/or
2. The best interest of the child.

The term "exigent circumstances" includes any placement of a child other than routine foster or licensed care situations.

14.2 Process & Procedure

The Department of Social Services Children's Division employee or juvenile court officer (JO) may request a name-based criminal history record check through MULES and NCIC to include active orders of protection and warrants from law enforcement. The inquiry QH using purpose code X is based on the applicant's name, date of birth, and social security number and will indicate if there is or is not criminal history indexed in III. Only with the submission of fingerprints is an applicant's identification and criminal history positively identified. When placement is made in response to an emergency child placement and purpose code X inquiry, fingerprint submission is required within 15 calendar days of placement. (Section 210.482 RSMo.)

For each MULES/NCIC inquiry, the ORI of the law enforcement agency is used. The purpose code must indicate "X," the reason field must indicate "emergency child placement," and the attention field or requestor must indicate, at a minimum, the "last name of the DSS-CD employee or JO."

The agency that initiates/requests the purpose code X inquiry is responsible to ensure fingerprints are submitted within 15 days in every instance when child placement occurred. An exception to the fingerprint requirement after child placement is when the applicant refuses to submit fingerprints. (Section 210.482.3 RSMo.)

14.3 Direct Terminal Access

Juvenile courts/officers that have direct MULES/NCIC terminal access may conduct an inquiry using purpose code X for emergency child placement for their own information or on behalf of a DSS-CD employee. Juvenile courts/officers without direct access to MULES/NCIC will contact their local law enforcement for the inquiry, and should follow the same procedure as the DSS-CD employee.

Steps to take prior to requesting criminal history (using purpose code X) for emergency child placement:

1. Contact your local law enforcement or JO (if the JO has direct terminal access) and ask if they are willing to provide this service to your circuit.
2. Provide a list of the DSS-CD employee names to law enforcement. This will help law enforcement identify persons that are authorized to request/receive criminal history.

14.3.1 Direct Terminal Access Procedure For Juvenile Court/Officer (JO)

1. ORI: MO026009T
2. Purpose Code: X
3. Reason Field: Emergency Child Placement
4. Attention/Requestor Field: Last name of requesting individual — this will be the JO name or CD worker name.

14.3.2 Direct Terminal Access Procedures For Law Enforcement

1. ORI: Law Enforcement personnel will enter their agency ORI (Criminal Justice ORI).
2. Purpose Code: X
3. Reason Field: Emergency Child Placement
4. Attention/Requestor Field: Last name of requesting individual — this will be the DSS-CD worker name or JO name.

14.4 Dissemination Procedures

Specific details of any hit notification may be provided to the DSS-CD employee from law enforcement or JO in two ways, depending on agency policy:

1. Over the phone
2. In hard copy (printed)

Prior to providing specific details of any hit notification over the phone, the identification of the requesting person, i.e. DSS-CD employee or JO, must be verified. Therefore, it is recommended that the DSS-CD employees take the appropriate steps to familiarize themselves with their local law enforcement and juvenile court officers. It is also recommended that a list of authorized CD employee names is provided to the local law enforcement agencies, ensuring that only authorized CD employees are requesting the inquiry.

The NCIC/MULES inquiry may include:

1. Active orders of protection
2. Outstanding warrants
3. Criminal history records/arrest information housed with the Patrol and FBI

Although a verbal statement of all information obtained from the inquiry is authorized, some law enforcement agencies may only choose to provide a "hit" or "no hit" response. In this instance, the DSS-CD employee may request a hard copy of the criminal history. When a printed copy is requested, it should be picked up in a timely manner.

When the results are requested in hard copy form, the DSS-CD employee must adhere to the following:

1. Appear in person at the law enforcement agency.
2. Produce a current state photo ID and/or DSS identification badge.
3. Sign a secondary dissemination log.

The NCIC/MULES inquiry is not based on fingerprints, and therefore, is not positive identification. The information must not be disclosed or disseminated to the subject of record or outside of Children's Division or Juvenile Court authorized personnel. The inquiry results should be destroyed when no longer needed.

14.5 Fingerprint Submission Requirement & Procedures

For each and every emergency child placement request (using a purpose code X inquiry) that resulted in a child placement, fingerprints must be submitted within 15 calendar days after placement.

1. Every effort must be taken by DSS-CD employees to ensure fingerprints are submitted to the MSHP-CJISD within the 15 calendar days after placement. Failure to comply will result in noncompliance.
2. In the event the child is removed from the home, even if the child was only placed for a limited time, fingerprints are still required.
3. The only exception to fingerprint submission is when the applicant refuses to submit fingerprints and the child was removed due to the refusal.

Fingerprint submission is the responsibility of the "requesting entity." If the emergency child placement was requested by the DSS-CD employee, DSS-CD is responsible for fingerprint submission. If the emergency child placement was requested by the JO, the JO is responsible for the fingerprint submission. It is recommended that DSS-CD employees and JOs have an agreement in place to ensure the fingerprint submissions are submitted timely.

14.5.1 Fingerprint Submission By DSS-CD

- ORI : MO920360Z
- Reason Fingerprinted (state law): Section 210.482 RSMo.
- OCA: DSS CD Circuit number.

The DSS-CD requires that all applicants submit fingerprints using the state contracted electronic vendor. In order to use the vendor, MACHS registration numbers have been assigned to each DSS-CD Circuit and to DSS Central Office. It is the responsibility of the DSS-CD to instruct applicants on fingerprint submission procedures and to ensure the appropriate four-digit registration number is used. (For MACHS and electronic fingerprint submission procedures, refer to Section 8.)

14.5.2 Fingerprint Submission By Juvenile Court/Officer

- ORI: Court ORI, ending in the letter "J"
- Reason Fingerprinted: Section 210.482 RSMo.
- OCA: N/A

Dissemination of the fingerprint-based results to the subject of record is authorized. When disseminating to the subject of record, it is recommended that a copy be made of the original results and marked as "copy." When picking up in person, the subject of record must show photo ID and must sign a secondary dissemination log. (Refer to Section 4 for more details on dissemination and destruction policy.)

14.6 Log Scan Report Procedure — DSS-CD

Log scan reports are generated monthly for every county and sent to the circuit managers. The reports show the names of persons queried for criminal history in response to emergency child placement (using purpose code X). Circuit managers and their staff are responsible for ensuring each inquiry was made for an authorized purpose and that fingerprint submission was obtained from each person when child placement occurred.

SECTION 15: Public Housing Authorities

15.1 Authority & Access

Pursuant to the National Housing Act of 1937, Title 42, USC, Section 1437d(q), the "Act," which was amended by the Housing Opportunity Program Extension Act of 1996 Public Law 104-120, and the Quality Housing and Work Responsibility Act of 1998, Public Law 105-276, administrators of Department of Housing and Urban Development (HUD) assisted housing programs (AHPs) are permitted to obtain criminal history records of current and prospective tenants receiving benefits under an AHP, for purposes of applicant screening, lease enforcement, and eviction, where applicable. On May 29, 1996, the HUD and the Department of Justice entered in an agreement which sets forth procedures for the access to criminal history data under the act.

The act, as amended, provides that a participating agency shall establish and implement a system of records management that ensures criminal records are maintained confidentially, not misused or improperly disseminated, and destroyed once the purpose for which the record was requested has been accomplished. The act also institutes criminal penalties for improper release of information as well as establishes civil liability for negligence.

In accordance with this agreement, state and local law enforcement agencies are allowed access through the NCIC System to the Interstate Identification Index for the purpose of determining whether a tenant of, or an applicant for, assisted housing may have a criminal history record indexed in the III. Access for this purpose does not entitle the requesting law enforcement agency to obtain the full content of automated records through III.

In order to receive authority for access to criminal history through NCIC System and III, the Public Housing Authority must request an Originating Agency Identifier through the FBI. Generally, ORI requests are sent to the MSHP-CJISD prior to being requested from the FBI; however, housing authorities are the exception. The ORI assignment request will be made directly to the FBI, and once approved, the FBI notifies the MSHP-CJISD. When the MSHP-CJISD is notified of the ORI, the ORI is added for access to the state and FBI systems and a Noncriminal Justice Agency User Agreement is sent to the Housing Authority for completion and return to the MSHP-CJISD.

All requests for ORI numbers should be sent directly to the FBI at the following address:

Chief, Programs Support Section
Module E3
FBI Complex
1000 Custer Hollow Road
Clarksburg, WV 26306

The request for ORI should include:

- The full name of the PHA;
- The PHA's complete mailing address;
- The county in which the PHA's main office is located;
- The number of fingerprint cards the PHA will initially need;
- The name and telephone number of the PHA contact person;
- The name of the CA or SIB the PHA will utilize to submit its fingerprint cards to the FBI;
- The FBI will assign an ORI number to the PHA and furnish applicant fingerprint cards to the PHA bearing that ORI number. A reorder form will be included with each supply of fingerprint cards so that the PHA can reorder with necessary.

NCIC ORI numbers, ending in "Q," are assigned to authorize Housing Authorities for identification purposes. When conducting inquiries, law enforcement agencies will use the ORI number assigned to the requesting Housing Authority. This ORI number serves as the authority for the Housing Authority and is required with each inquiry performed by law enforcement and with each fingerprint submission.

Public Law 104-120 provides that the "National Crime Information Center, police departments, and other law enforcement agencies shall, upon request, provide information to public housing agencies regarding the criminal conviction records of adult applicants for, or tenants of, public housing for purposes of applicant screening, lease enforcement, and eviction. The FBI has established purpose code H for housing, to be used when requesting a name search (QH) of III under the authority of Public Law 104-120. purpose code H is valid only for QH inquiries when those inquiries are made for a Public Housing Authority. (NCIC Technical and Operational Update, FBI CJIS Division Informational Letter, dated Dec. 6, 1996)

The inquiry will include:

- Housing Authority ORI
- Inquiry of QH
- Purpose Code of H.

Only a "hit or no hit" response from law enforcement is authorized — specific details of what the criminal history may indicate is strictly prohibited.

The QH response will provide a list of all individuals included in III whose name and personal descriptors match those included in the inquiry. The state or local law enforcement agency is authorized to inform a Public Housing Authority if a name check reveals that a public housing applicant or tenant may have a criminal history record indexed in III. To obtain a copy of the criminal history record, the Public Housing Authority must submit a completed fingerprint card on the applicant or tenant. The Public Housing Authority will receive the criminal history record only after a positive identification, based on fingerprints, has been made.

15.2 Criminal History Record Inquiry & Fingerprint Submission Process

1. Housing Authority applies for an ORI from the FBI.
2. Housing Authority is assigned an ORI, ending with the letter "Q."
3. Housing Authority contacts their local law enforcement agency and enters into a "non-terminal user agreement" for criminal history inquiries by law enforcement through direct (MULES/NCIC) terminal access.
4. The PHA submits a name check request to the law enforcement agency. The name check request must include the name, date of birth, and social security number of the applicant/resident (if he/she has one).
5. Using the ORI assigned to the PHA, the law enforcement agency will access the III through the NCIC to determine whether an applicant/resident for public housing may have a criminal history record.
6. The law enforcement agency is authorized to give a "hit or no hit" notification — a hit notification means that the information given may match a criminal record indexed in the national database. This statement means only that based on the information provided, the record may belong to the applicant/resident, but is inconclusive without a positive fingerprint comparison. The results of an inconclusive name check cannot be used to deny an applicant's admission to housing or as a basis to evict a tenant.
7. For positive hit notifications, the Housing Authority must notify the applicant that fingerprints are needed in order to verify criminal history and receive the full content of the record, if one does exist.
8. The Housing Authority will give the applicant an Applicant Fingerprint Card (FD-258) which has the Housing Authority ORI pre-printed or written on the card. The "reason fingerprinted" field should indicate "housing." (In some instances, where applicable, law enforcement agencies may use their livescan devices for electronic capture of fingerprints. The Housing Authority ORI must be used and an "Authorization To Invoice" must be on file with MSHP-CJISD prior to electronic transmission.)
9. The applicant will take the fingerprint card to their local law enforcement to be inked and then return the completed fingerprint card to the Housing Authority.
10. The Housing Authority should verify that the fingerprint card is completed in full and then mails the fingerprint card with appropriate fees to the MSHP-CJISD for processing.
11. The applicant's or tenants fingerprints will be compared with criminal fingerprints maintained in FBI files; and, if found to be identical, a copy of the corresponding criminal history record will be provided to the PHA.
12. The results of the background check are mailed from the MSHP-CJISD to the Housing Authority.

The Housing Authority may submit fingerprint cards either directly to the FBI or to the responsible State Identification Bureau, providing the SIB has agreed to process the cards. The MSHP-CJISD processes fingerprint cards for state and FBI criminal history responses for Public Housing Authorities in Missouri.

It is important to note that, based on Public Law 104-120, the inquiry information is provided to the Housing Authority only to inform them of the probable existence or nonexistence of a criminal history

record. The Housing Authority will use the results of the response as a factor in deciding if a fingerprint-based search of criminal history is needed. Only with the submission of fingerprints can a positive identification be made and a record provided, if such a record exists. Therefore, the result of the inquiry should not be used as the basis for disqualification, lease enforcement, or eviction.

If the state or local law enforcement agency informs the Housing Authority that the inquiry reveals no additional information, the Housing Authority need not pursue further inquiries.

15.3 Non-terminal Agency User Agreements

All Housing Authorities with an ORI must have a non-terminal user agreement with the local law enforcement agency that will perform the name-based queries for them. Housing Authorities that have an approved ORI should contact their local law enforcement agency to establish procedures for requesting inquiries.

When the non-terminal user agreement is in place between the Housing Authority and the law enforcement agency, inquiries based on an applicant's personal identifiers may be performed through MULES and NCIC.

SECTION 16: Concealed Carry Permits

16.1 Access & Use

Law enforcement agencies, unlike noncriminal justice agencies, have the unique role of accessing criminal history record information for criminal justice purposes, i.e. the administration of criminal justice functions, and also for noncriminal justice purposes. The information contained in this section applies to law enforcement agencies that have the responsibility of issuing concealed carry permits.

Although issuing concealed carry permits is a noncriminal justice function, the process of obtaining criminal history for the required background checks is authorized two ways:

1. Fingerprint submission for positive identification, and
2. Direct terminal access of MULES/NCIC inquiries based on the applicant's personal identifying information.

Individuals applying for a concealed carry permit are required to submit fingerprints to the law enforcement agency in their county (county or city sheriff) for submission to the MSHP and FBI prior to the law enforcement agency issuing such permit. The statute requires that both a state and FBI background check be completed as one of the requirements in the screening process. For a complete list of the requirements to obtain a concealed carry permit, refer to Sections 571.101 through 571.121 RSMo.

The importance of obtaining a fingerprint background check is twofold:

1. As with any screening based on positive identification, a fingerprint submission is the most reliable method of ensuring that the law enforcement agency is obtaining the actual record of the person that is applying for the permit.
2. It is the only method that will ensure a complete and accurate record of arrests and prosecutions. The disqualifiers that would prohibit the issuance of a permit would require the most complete and up-to-date information about an applicant's criminal history, so that the permit issuing agency may make an accurate determination.

16.2 Fingerprint Submission

Law enforcement agencies that have a livescan (electronic) fingerprint device are authorized to transmit the fingerprints and personal information for an applicant applying for a concealed carry permit. The agency will use the "Applicant Format" on the livescan device.

For livescan submission, the agency must ensure:

1. The agency ORI is used in the ORI field.
2. The agency ORI is also entered in the OCA field.
3. The "Reason Fingerprinted" field must indicate "571.101," which refers to that section in the state statutes.
4. The record type for transmission must be "X" for state and FBI, and fees apply.
5. Prior to livescan transmission, the agency must first submit an "Authorization To Invoice" to the MSHP-CJISD to establish billing.
6. Fees for conceal carry permits are referenced in Section 43.530 RSMo. Both state and FBI fees apply.

Some agencies with a livescan choose not to transmit and will print the completed fingerprint card for mailing to the MSHP-CJISD. Some may also choose to ink applicants for manual submission to the MSHP-CJISD. These methods of submission are acceptable.

16.3 National Instant Criminal Background Check System (NICS)

In addition to a fingerprint background check, all applicants are subject to a name search through the National Instant Criminal Background Check System. This database was established as part of the Brady Handgun Violence Prevention Act of 1993 (Public Law 103-159 Brady Handgun Violence Prevention Act of 1993) and is a national system that cross-references NCIC, III, and the NICS index to search for individuals that are, by federal law, prohibited from receiving firearms. While access to this database has been previously available to law enforcement agencies, the NICS name check is now a mandatory part of the concealed carry permit screening process. (Missouri Senate Bill No. 75)

The transaction or inquiry into MULES is performed by entering the query of QNP with a purpose code 14. For positive "hit" notifications, the query QMH with purpose code F should be entered to receive the criminal history. Law enforcement agencies needing assistance with the transaction/inquiry into MULES for NICS checks should contact their local regional MULES trainer. (Purpose code 14 replaced purpose code P pursuant to NCIC notification dated 1/9/2012.)

While the NICS is not based on positive identification, a NICS inquiry does act as an added layer of screening that may prevent the issuance of a concealed carry permit due to other disqualifiers that may not appear on an applicant's criminal history.

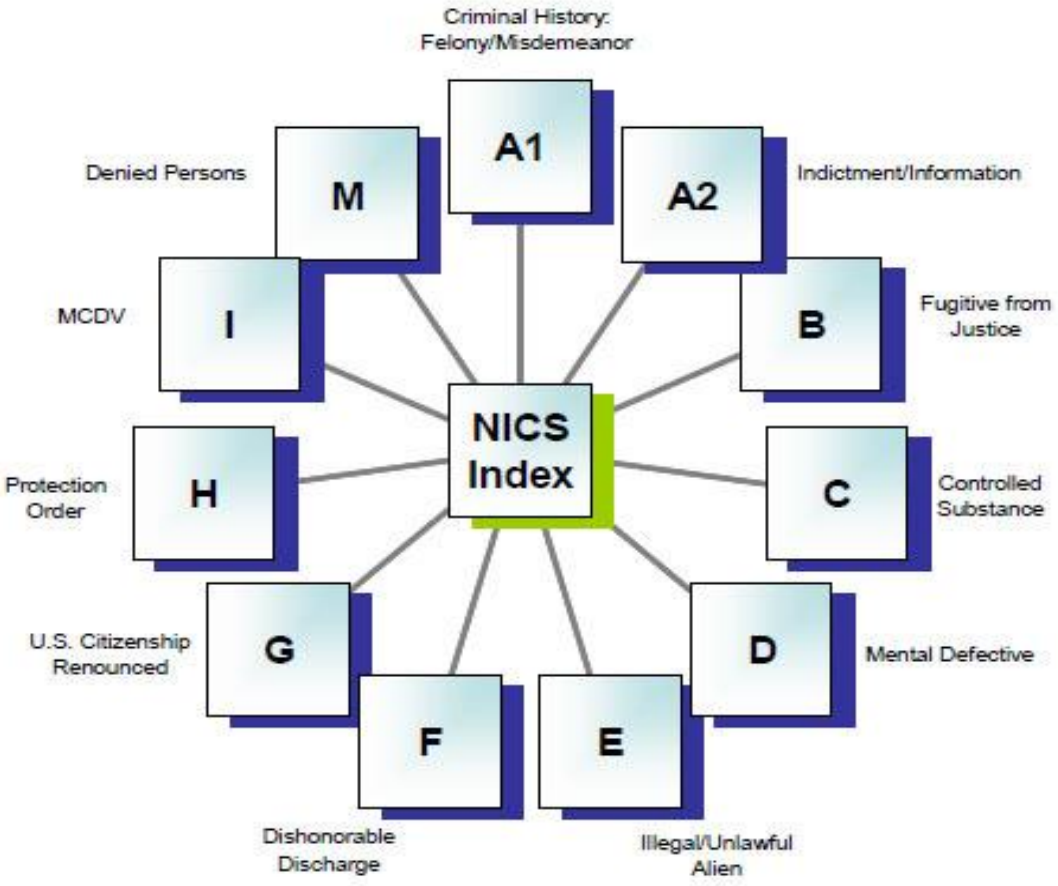
The following entries in the NICS system are good examples of federal disqualifiers that are unrelated to criminal history and would not be present on an applicant's fingerprint background check or name check performed by law enforcement based solely on arrest and prosecution information:

1. Names provided by the Veterans Administration of those adjudicated as mentally incompetent or dishonorably discharged;
2. Mental health records from institutions, psychiatrists, police departments, family members;
3. Juveniles adjudicated as delinquent or escaped custody without arrest warrants issued;
4. Individuals with Canadian offenses;
5. Members of violent criminal gangs;
6. Members of terrorist organizations;
7. Persons illegally or unlawfully in the United States; and
8. Prior United States citizen who has renounced citizenship.

The above list mirrors many of the state disqualifiers as contained in statute and will aid the law enforcement agency in ensuring that the most complete background screening has been conducted prior to issuing a permit. For more information about NICS, go to the FBI's website. (See Appendix E.)

Below are codes that may appear upon a positive response to a NICS inquiry:

A1 Criminal History Felony/Misdemeanor
A2 Indictment/Information
B Fugitive from Justice
C Controlled Substance
D Mental Defective
E Illegal/Unlawful Alien
F Dishonorable Discharge
G U.S. Citizenship Renounced
H Protection Order
I MCDV (Misdemeanor Crime Domestic Violence)
M Denied Persons


Criminal History: Felony/Misdemeanor
A1
A2
Indictment/Information
B
Fugitive from Justice
C
Controlled Substance
D
Mental Defective
E
Illegal/Unlawful Alien
F
Dishonorable Discharge
G
U.S. Citizenship Renounced
H
Protection Order
I
MCDV
M
Denied Persons
NICS Index

16.4 NICS Appeals & Voluntary Appeal File (VAF)

According to the NICS 2012 Operations Report, 1.01 percent of the 2012 NICS inquiries resulted in a final transaction denial. If a person believes that they have been wrongfully denied through a NICS background check, the applicant may file an appeal request to the FBI Criminal Justice Information Services (CJIS) Division's NICS Section. The applicant will be asked to submit fingerprints for identity verification to determine if the disqualifying record belongs to the applicant.

The primary reason for overturned denials in 2012 was that the applicant's fingerprints did not match the disqualifying subject's fingerprints. Individuals requesting an appeal for a NICS denial are encouraged to go to the NICS appeal website: www.fbi.gov/about-us/cjis/nics/appeals/nics-appeals-process/appeals-home

16.5 Challenging A Criminal History Record vs. Challenging A NICS Appeal

Appealing a NICS denial should not be confused with an applicant's right to challenge their criminal history record information as discussed in Section 3, Applicant Privacy Rights. All noncriminal justice applicants have the right to update or challenge their fingerprint-related criminal history. For example, if the permit issuing law enforcement agency is denying an applicant due to adverse criminal history and the applicant believes the information to be inaccurate, federal privacy laws ensure that the applicant has the opportunity to complete or correct their record.

While a NICS denial may be based on adverse criminal history, other factors may also be contributing to a NICS denial. The NICS inquiry is name-based and for this reason, the appeal process will involve the submission of fingerprints to establish whether the applicant's fingerprints match those of the disqualifying subject within the NICS database.

16.6 Policy Compliance Reviews

Law enforcement agencies that issue concealed carry permits are subject to Noncriminal Justice Policy Compliance Reviews due to access to criminal history record information received for noncriminal justice purposes. The PCR focuses on the use, retention, dissemination, destruction, and security of the criminal history. (See Section 6 — Agency Audits.)

Agencies issuing a concealed carry permit will be held to the same rules and regulations governing access to criminal history as other noncriminal justice agencies; however, below are some PCR areas that are specific to law enforcement agencies issuing concealed carry permits.

16.7 Dissemination Of CHRI

16.7.1 Subject Of Record — Law enforcement agencies issuing conceal carry permits have different requirements than most noncriminal justice agencies regarding dissemination.

Most agencies, depending on agency policy, have the option to disseminate to the subject of the record. (Title 5 USC Section 552a, Privacy Act of 1974)

When a permit request is being denied, law enforcement agencies must:

1. Notify the applicant in writing of the reason for a denial.
2. If the denial is based on adverse criminal history, the law enforcement agency is required to disseminate the criminal history record information (state and FBI) to the subject of record.

When disseminating the criminal history record responses (state and FBI) to the applicant, it is recommended that a copy be made and stamped as "copy." When the applicant is appearing in person to pick up the denial letter and criminal history, the applicant should show positive ID and sign the secondary dissemination log. When dissemination is through written correspondence mailed to the applicant, the secondary dissemination log should indicate mailed.

The written notification letter to the applicant may also serve as a dissemination log for that record. The law enforcement agency may choose to keep individual dissemination logs or computerized logs. Whatever method of dissemination, all pertinent information must be recorded and the dissemination records will be viewed during the PCR. (See Section 4, Dissemination.)

To assist law enforcement agencies with the requirement of written notification to the applicant for permit denials, the MSHP CJIS Division has a sample letter that incorporates all of the statute requirements. (See Appendix E.)

16.7.2 Dissemination Between Issuing Agencies (Law Enforcement To Law Enforcement).
Dissemination between law enforcement agencies is authorized, but it not required. For example:

- If law enforcement agency in county A issues a conceal carry permit to an applicant who then moves to county B, the law enforcement agency in county B may request a copy of the fingerprint background check from county A.
- If county A agrees to disseminate the results to county B, a dissemination log entry is required.
- County B may use the record for the purpose(s) as indicated in statute. Any other purpose is not authorized.
- As a precaution, the MSHP-CJISD discourages the re-use of criminal history as the record will not be the most current available for the applicant. (Title 28 CFR 50.12 and Title 28 CFR 20.33)
- Although not a violation of law, when a new need arises, a new criminal history should be obtained to ensure the most current information is available.

16.8 Dissemination Logs

Whether disseminating criminal history for law enforcement purposes or for concealed carry permits, dissemination log requirements are the same. However, for dissemination based on concealed carry permits, it is recommended that law enforcement agencies keep a separate log since the retention and auditors are different. (See Section 4, Dissemination Log Standards.)

16.9 PCR Conversation Examples

1. *Auditor Question:* Does your agency store concealed carry permit information in record management software, such as ITI?
Authorized Recipient Answer: Yes.
Auditor Response: If your agency stores criminal history related to concealed carry permits in an electronic medium, this is considered electronic storage and will be subject to audit for security and access.

2. *Auditor Question*: Is the CHRI stored on a server maintained in-house or offsite?
AR Answer: Yes/No.
Auditor Response: Increasingly, agencies are using web-based server or storage options. If CHRI is stored electronically, it is important to know where your server is maintained and take the appropriate steps to prevent any unauthorized access.

3. *Auditor Question*: Your agency has agreed to provide an applicant with a copy of his/her criminal history. May a family member, upon the request of the applicant, stop by to pick up the record for the applicant?
AR Answer: Yes/No.
Auditor Response: No. While it is acceptable to disseminate to the applicant, it is not acceptable to disseminate to any other person, even with permission from the applicant.

4. *Auditor Question:* Your agency has submitted fingerprints on an applicant and has received a state response, but the FBI rejected the prints due to poor quality. What do you do?
AR Answer: The AR might not know or might provide the same as the "auditor response" below.
Auditor Response: An FBI rejection is not a proper federal response on a background check. Even if the rejection is due to poor quality, a second fingerprint submission is required and is at no additional cost, if resubmitted correctly. Should the prints be rejected a second time, the agency has the ability to request a name check through the FBI. (See Section 8, Fingerprint Submission Procedures.)

5. *Auditor Question*: Your agency uses an offsite location to store the hard copy criminal history responses. Is this authorized?
AR Answer: The AR might not know or might provide the same as the "auditor response" below.
Auditor Response: No, unless an Outsourcing Standard is approved prior to off-site storage. Once criminal history leaves the control of your agency, you are allowing a third-party to have access.

This is not authorized without first implementing an Outsourcing Standard. (See Section 7, Security and Management Control Outsourcing Standard)

To access concealed carry permit applications, renewal forms, or for questions about the issuance of a permit, please contact the Missouri Sheriff's Association at www.mosheriffs.com

Applicable statutes for concealed carry permits are found in Sections 571.101 through 571.121 RSMo. Please refer to http://www.moga.mo.gov/mostatutes/statutesAna.html

APPENDIX A — CJIS AUDITOR / TRAINER CONTACT INFORMATION

The Noncriminal Justice (NCJ) Audit and Training Team consists of three individuals who provide statewide training and conduct compliance reviews. The team is managed by one supervisor/manager and reports to an assistant director. They are assigned to the Missouri State Highway Patrol General Headquarters in Jefferson City.

NCJ Audit & Training Team
(573) 526-6153

Team Manager/Supervisor
Mr. Kerry K. Creach, CJIS Program Manager ext. 2646
Email: Kerry.Creach@mshp.dps.mo.gov

Region 1
Ms. Linda S. Lueckenhoff, CJIS Auditor/Trainer III ext. 2630
Email: Linda.Lueckenhoff@mshp.dps.mo.gov
(Kansas City area, Northwest and Western Counties)

Region 2
Ms. Valerie Hampton, CJIS Auditor/Trainer III ext. 2655
Email: Valerie.Hampton@mshp.dps.mo.gov
(Jefferson City area, Central, North/South Central Counties)

Region 3
Ms. Pamela Aberle, CJIS Auditor/Trainer III ext. 2625
Email: Pamela.Aberle@mshp.dps.mo.gov
(St. Louis area, East and Southeast Counties)

Region 4
Mr. Scott Schlueter, CJIS Auditor/Trainer II ext. 2653
Email: Scott.Schlueter@mshp.dps.mo.gov
(Springfield area, South and Southwest Counties)

CJIS Division Main Number

(573) 526-6153

CJIS Division Director, Captain Larry W. Plunkett Jr.	(573) 526-6160
CJIS Division Assistant Director, Lieutenant Steven J. Frisbie	(573) 522-4968

Civil Processing & Compliance Section

Mr. Kerry K. Creach, CJIS Program Manager	ext. 2646
Ms. Carol Kampeter, Section Supervisor	ext. 2617
CJIS Quality Control For assistance with criminal history, RAP sheets, Dispositions, MACHS fingerprint website	Select Option 3, then Option 2
Expungements	ext. 2649
Public Window (background checks)	ext. 2647/2644/2676
Missouri VECHS Program Enrollment	ext. 2647

MSHP CJIS Division Location — Annex Building

Physical Location
MSHP CJIS Division
Annex Building
1510 E. Elm Street
Jefferson City, MO 65101

Mailing Address
MSHP CJIS Division
P.O. Box 9500
Jefferson City, MO 65102-9500

APPENDIX B: ACRONYMS

AFIS — Automated Fingerprint Identification System

APB — Advisory Policy Board

AR — Authorized Recipient

CFR — Code of Federal Regulations

CHRI — Criminal History Record Information

CJI — Criminal Justice Information

CJIS — Criminal Justice Information Services

CJISD — Criminal Justice Information Services Division

CSA — CJIS Systems Agency

CSO — CJIS Systems Officer

DOJ — Department of Justice

FIPS — Federal Information Processing Standard

FBI — Federal Bureau of Investigation

IAFIS — Integrated Automated Fingerprint Identification System

ICTD — Information & Communications Technology Division

III — Interstate Identification Index

ISO — Information Security Officer

LASO — Local Agency Security Officer

MACHS — Missouri Automated Criminal History Site

MSHP — Missouri State Highway Patrol

MULES — Missouri Uniform Law Enforcement System

NCIC — National Crime Information Center

NCJA — Noncriminal Justice Agency

NCPA — National Child Protection Act

NGE — Nongovernmental Entity

NICS — National Instant Criminal Background Check System

NFF — National Fingerprint File

OCA — Originating Case Agency

OCN — Offense Cycle Number

ORI — Originating Agency Identifier

PCR — Policy Compliance Review

POC — Point of Contact

RAP — Record of Arrest & Prosecution

RSMo. — Revised Statutes of Missouri

SAT — Security Awareness Training

SIB — State Identification Bureau

SID — State Identification Number

TCN — Transaction Control Number

USC — United States Code

VCA — Volunteers for Children Act

VECHS — Volunteer and Employee Criminal History Service

APPENDIX C: TERMS & DEFINITIONS

These definitions are derived from the CJIS Security Policy, Title 28 CFR Section 20.3, the National Crime Prevention and Privacy Compact Council (Compact), and the Revised Statutes of Missouri.

Access to CJI — The physical or logical (electronic) ability, right, or privilege to view, modify, or make use of criminal justice information.

Administration of Criminal Justice — The performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal history information, including fingerprint searches, photographs, and other indicia of identification.

Arrest — An actual restraint of the person of the defendant, or by his or her submission to the custody of the officer, under authority of a warrant or otherwise for a criminal violation which results in the issuance of a summons or the person being booked.

Arrest Report — A record from a law enforcement agency of an arrest and of any detention or confinement incident thereto together with the charge therefore.

Asynchronous — In programming, those events occurring independently of the main program flow. The actions are executed in non-blocking scheme, allowing the main program flow to continue processing.

Audit — The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

Authorized Recipient — (1) A criminal justice agency or federal agency authorized to receive CHRI pursuant to federal statute or executive order; (2) A nongovernmental entity authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes; or (3) A government agency authorized by federal statute or executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

Authorized State Agency — A division of state government or an office of state government designated by the statutes of Missouri to issue or renew a license, permit, certification, or registration of authority to a qualified entity.

Background Check — A check of all appropriate information sources to include a state of residency and national tenprint-based (fingerprints) record check.

Care — Refers to the provision of care, treatment, education, training, instruction, supervision, or recreation.

Central Repository — The Missouri State Highway Patrol Criminal Justice Information Services Division, which is responsible for compiling and disseminating complete and accurate criminal history records, and for compiling, maintaining, and disseminating criminal incident and arrest reports and statistics.

Channeler – An FBI approved contractor, who has entered into an agreement with an authorized recipient(s), to receive noncriminal justice applicant fingerprint submissions and collect the associated fees. The channeler ensures fingerprint submissions are properly and adequately completed, electronically forwards fingerprint submissions to the FBI's CJIS Division for national noncriminal justice criminal history record check, and receives electronic record check results for dissemination to authorized recipients. A channeler is essentially an "expediter" rather than a user of criminal history record check results.

Child — Any person, regardless of physical or mental condition, under 18 years of age.

Children's Services Providers & Agencies — Any public, quasi-public, or private entity with the appropriate and relevant training and expertise in delivering services to children and their families as determined by the DSS-CD, and capable of providing direct services and other family services for children in the custody of the DSS-CD, or any such entities or agencies that are receiving state moneys for such services.

CJIS Audit Unit (CAU) — The organization within the FBI CJIS Division responsible to perform audits of CSAs to verify compliance with the CJIS Security Policy.

CJIS Security Policy — The FBI CJIS Security Policy document as published by the FBI CJIS ISO.

CJIS Systems Agency (CSA) — A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJIS data from various systems managed by the FBI CJIS Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies' connection to the FBI CJIS systems.

CJIS Systems Officer (CSO) — An individual located within the CJIS Systems Agency responsible for the administration of the CJIS network on behalf for the CJIS Systems Agency.

Compact Council — The entity created by the National Crime Prevention and Privacy Compact of 1998 that has the authority to promulgate rules and procedures governing the use of the III system for noncriminal justice purposes.

Confidentiality — The concept of ensuring that information is observable only to those who have been granted authorization to do so.

Confidential Information — Information maintained by the state agency that is exempt from disclosure under the provisions of the Public Records Act or other applicable state or federal laws. The controlling factor for confidential information is dissemination. Criminal history record information is protected by federal legislation.

Contemporaneously — Existing, occurring, or originating during the same time period.

Contractor — A private business, agency, or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a criminal justice agency or a noncriminal justice agency. Also, a private business approved by the FBI CJIS Division to contract with noncriminal justice agencies to perform noncriminal justice functions associated with civil fingerprint submission for hiring purposes.

Criminal History Records — (1) Information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising there from, including acquittal, sentencing, correctional supervision, or release; and (2) does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.

Criminal History Record Information (CHRI) — Information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition arising there from, sentencing, correctional supervision, and release.

Criminal History Record Information System — A system including the equipment, facilities, procedures, agreements, and organizations thereof for the collection, processing, preservation, or dissemination of criminal history record information.

Criminal Justice — Activities relating to the detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice includes criminal identification activities and the collection, storage, and dissemination of criminal history records.

Criminal Justice Agency — (1) Courts, and (2) a governmental agency or any subunit thereof that performs the administration of criminal justice pursuant to a statute or executive order, and that allocates a substantial part of its annual budget to the administration of criminal justice. Inspector General offices (state and federal) are included.

Criminal Justice Information (CJI) — Criminal justice information is the abstract term used to refer to all the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws including, but not limited to, biometric, identity history, person, organization, property, and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for noncriminal justice/civil agencies to perform their mission; including, but not limited to, data used to make hiring decisions.

Criminal Justice Information Services Division (CJIS) — The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Degauss — Neutralize a magnetic field to erase information from a magnetic disk or other storage device. In the field of information technology, degauss has become synonymous with erasing information whether or not the medium is magnetic. In the event the device to be degaussed is not magnetic (e.g. solid state drive, USB storage device), steps other than magnetic degaussing may be required to render the information irretrievable from the device.

Direct Access — (1) Having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Chapter 1, and Part 20). (2) Having the authority to query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

Disposition — Information disclosing that criminal proceedings have been concluded and the nature of the termination, including information disclosing that the police have elected not to refer a matter to a prosecutor or that a prosecutor has elected not to commence criminal proceedings; or disclosing that proceedings have been indefinitely postponed and the reason for such postponement. Dispositions shall include, but shall not be limited to, acquittal, acquittal by reason of insanity, acquittal by reason of mental incompetence, case continued without finding, charge dismissed, charge dismissed due to insanity, charge dismissed due to mental incompetency, charge still pending due to insanity, charge still pending due to mental incompetence, guilty plea, nolle prosequi, no paper, nolo contendere plea, convicted, youthful offender determination, deceased, deferred disposition, dismissed-civil action, found insane, found mentally incompetent, pardoned, probation before conviction, sentence commuted, adjudication withheld, mistrial-defendant discharged, executive clemency, placed on probation, paroled, or released from correctional supervision.

Dissemination — The transmission or distribution of CJI to authorized recipients.

Dissemination Log — Paper or automated log that records the transfer or release of criminal history record information.

Exigent Circumstances — A sudden unexpected event that results in an apparent risk to the health and safety of an individual that necessitates immediate action on the part of the state to provide protection to that individual.

FBI (Federal Bureau of Investigation) – An agency within the Department of Justice responsible for protecting and defending the United States against terrorist and foreign intelligence threats, upholding and enforcing the criminal laws of the United States, and providing leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

FBI CJIS Advisory Policy Board (APB) — The governing organization within the FBI CJIS advisory process comprised of representatives from criminal justice and national security agencies within the United

States. The APB reviews policy, technical, and operational issues relative to FBI CJIS Division programs and makes subsequent recommendations to the director of the FBI.

Final Disposition — Formal conclusion of a criminal proceeding at whatever stage it occurs in the criminal justice system.

Inactive — An investigation in which no further action will be taken by a law enforcement agency or officer for any of the following reasons: (a) a decision by the law enforcement agency not to pursue the case; (b) expiration of the time to file criminal charges pursuant to the applicable statute of limitations, or 10 years after the commission of the offense; whichever date occurs earliest; or, (c) finality of the convictions of all persons convicted on the basis of the information contained in the investigative report, by exhaustion of or expiration of all rights of appeal of such persons.

Information Security Officer (ISO) — Typically a member of an organization who has the responsibility to establish and maintain information security policy, assess threats and vulnerabilities, perform risk and control assessments, oversee the governance of security operations, and establish information security training and awareness programs. The ISO usually interfaces with security operations to manage implementation details and with auditors to verify compliance to established policies.

Integrated Automated Fingerprint Identification System (IAFIS) — The national fingerprint and criminal history system maintained by the FBI CJIS Division that provides the law enforcement community with automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.

Integrity — The perceived consistency of expected outcomes, actions, values, and methods of an individual or organization. As it relates to data, it is the concept that data is preserved in a consistent and correct state for its intended use.

Interstate Identification Index System (III System) — The cooperative federal-state system for the exchange of criminal history records, and includes the National Identification Index, the National Fingerprint File, and, to the extent of their participation in such system, the criminal history record repositories of the states and the FBI.

Local Agency Security Officer (LASO) — The primary information security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to information security, disseminates information security alerts and other material to their constituents, maintains information security documentation (including system configuration data), assists with information security audits of hardware and procedures, and keeps the CSA informed as to any information security needs and problems. For noncriminal justice purposes, the LASO serves in the same capacity although FBI CHRI is received based on fingerprints and not through direct terminal access.

Missouri Charge Code — A unique number assigned by the Office of State Courts Administrator to an offense for tracking and grouping offenses.

Missouri Criminal Record Review — A review of criminal history records and sex offender registration records pursuant to Sections 589.400 to 589.425 RSMo.

MULES — Missouri Uniform Law Enforcement System is a statewide-computerized communications system provided by the Patrol designed to provide services, information, and capabilities to the law enforcement and criminal justice community in the state of Missouri.

National Crime Information Center (NCIC) — The computerized information system, which includes telecommunications lines and any message switching facilities that are authorized by law, regulation, or policy approved by the attorney general of the United States to link local, state, tribal, federal, foreign, and international criminal justice agencies for the purpose of exchanging NCIC-related information. The NCIC includes, but is not limited to, information in the III System.

National Criminal Record Review — Review of the criminal history records maintained by the Federal Bureau of Investigation.

National Instant Criminal Background Check System (NICS) — A system mandated by the Brady Handgun Violence Prevention Act of 1993 that is used by federal firearms licensees (FFLs) to instantly determine via telephone or other electronic means whether the transfer of a firearm would be in violation of Section 922 (g) or (n) of Title 18, United States Code, or state law, by evaluating the prospective buyer's criminal history.

nolle prossed – A formal notice of abandonment by a plaintiff or prosecutor of all or part of a suit or action.

Noncriminal Justice Agency (NCJA) — A governmental or non-governmental agency, or any subunit thereof, that provides services primarily for purposes other than the administration of criminal justice. Examples of services include, but not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

Non-Criminal Justice Purposes — The use of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

Outsourcing — The process of delegating in-house operations to a third-party. For instance, when the administration of criminal justice functions (network operations, dispatch functions, system administration operations, etc.) are performed for the criminal justice agency by a city or county information technology department or are contracted to be performed by a vendor.

Outsourcing Standard — The National Crime Prevention and Privacy Compact Council Outsourcing Standard provides uniform standards and processes for the interstate and federal-state exchange of criminal history records for noncriminal justice purposes.

Personally Identifiable Information (PII) — Information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when

combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

Positive Identification — A determination, based upon a comparison of fingerprints or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III system. Identifications based solely upon a comparison of subject's name or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.

Provider — A person who has or may have unsupervised access to children, the elderly, or persons with disabilities, and is employed by or seeks employment with a qualified entity, or volunteers or seeks to volunteer with a qualified entity, or owns or operates a qualified entity.

Qualified Entity — A person, business, or organization, whether public or private, for profit, not for profit, or voluntary, that provides care, placement, or educational services for children, the elderly, or persons with disabilities as patients or residents, including a business or organization that licenses or certifies others to provide care or placement services.

RAP Back — An IAFIS service that allows authorized agencies to receive notification of subsequent criminal activity reported to the FBI and committed by persons of interest.

Secondary Dissemination — Re-dissemination of FBI CJIS data or records from an authorized agency that has direct access to the data to another authorized agency.

Shredder — A device used for shredding documents, often as a security measure to prevent unapproved persons from reading them. Strip-cut shredders, also known as straight-cut or spaghetti-cut, slice the paper into long, thin strips, but are not considered secure. Cross-cut shredders provide more security by cutting paper vertically and horizontally into confetti-like pieces.

State — Any state of the United States. For the purpose of this CJIS–NCJ Policy Manual, the word state refers specifically to Missouri.

State Compact Officer — The representative of a state that is party to the National Crime Prevention and Privacy Compact, and is the chief administrator of the state's criminal history record repository, or a designee of the chief administrator who is a regular full-time employee of the repository.

State Identification Bureau (SIB) — The state agency with the responsibility for the state's fingerprint identification services.

State Offense Cycle Number — A unique number, supplied by or approved by the Missouri State Highway Patrol, on the state criminal fingerprint card. The offense cycle number (OCN) is used to link the identity of a person, through fingerprints, to one or many offenses for which the person is arrested

or charged. The OCN will be used to track an offense incident from the date of arrest to the final disposition when the offender exits from the criminal justice system.

Statute — An act of congress or of a state legislature or a provision of the Constitution of the United States or of a state.

User Agreement – A terms-of-service agreement that must be signed prior to accessing CJI. This agreement is required by each CJA and NCJA, and spells out user's responsibilities, the forms and methods of acceptable use, penalties for their violation, disclaimers, and so on.

APPENDIX D: LAWS

This section is for reference only and may not be all inclusive of laws that grant access to CHRI.

REVISED STATUTES OF MISSOURI

Chapter 43 – Criminal Records, Central Repository

Section 43.500 RSMo. — Definitions.

Section 43.527 RSMo. — Payment for records, exceptions.

Section 43.530 RSMo. — Fees, method of payment — Criminal Record System Fund, established — fund not to lapse.

Section 43.532 RSMo. — Use of records, limitations, — authority of Central Records Repository to retain information — unlawful obtaining of information penalty.

Section 43.535 RSMo. — Municipal and county government, MULES criminal record review permitted, fee — fingerprinting, when — confidentiality.

Section 43. 540 RSMo. — Criminal records review — definitions — Patrol to conduct review, when, procedures, confidentiality, violations, penalty — Patrol to provide forms.

Section 43.542 RSMo. — Approval of National Crime Prevention and Privacy Compact — Execution of Compact.

Section 43.543 RSMo. — Certain agencies to submit fingerprints, use of fingerprints for background search — procedures for submission.

Section 43.546 RSMo. — Fingerprinting of applicants for background checks permitted by state agencies, boards, and commissions, when — procedures.

Section 43.547 RSMo. — Gubernatorial appointees, fingerprint background checks required — procedures.

Chapter 67 — Political Subdivisions, Miscellaneous Powers — Regional Taxicab Districts (St. Louis)

Section 67.1818 RSMo. — Licensure, taxicab code to include administrative procedures.

Section 67.1819 RSMo. — Background checks required, when — payment of fees.

Chapter 168 — Personnel — Teachers & Others

Section 168.071 RSMo. — Revocation, suspension, or refusal of certificate or license, grounds, procedure, and appeal.

Section 168.133 RSMo. — Criminal background checks required for school personnel, when, procedures — rulemaking authority.

Chapter 192 — Department of Health and Senior Services

Section 192.2495 RSMo. – Until December 31, 2016 — Criminal background checks of employees, required when — persons with criminal history not to be hired, when, penalty — failure to disclose, penalty— improper hirings, penalty — definitions — rules to waive hiring restrictions.

Section 192.2495 RSMo. – Beginning January 1, 2017 — Criminal background checks of employees, required when — persons with criminal history not to be hired, when, penalty — failure to disclose, penalty — improper hirings, penalty — definitions — rules to waive hiring restrictions.

Criminal background checks of employees ... if applicant has not lived in this state for five consecutive years. (Formerly Section 660.317)

NOTE: House Bill 1299 changed the laws associated with the Department of Social Services and the Department of Health and Senior Services. The Division of Aging within the Department of Social Services was transferred by executive order in 2001, to the Department of Health and House Bill 1299 updates Missouri law to reflect this organizational change. The bill eliminates the Division of Aging within the Department of Social Services and transfers the authority and duties to the Department of Health and Senior Services. As a result, Section 660.317 RSMo. was repealed and Section 192.2495 RSMo. was enacted in lieu thereof. (August 2014)

Chapter 210 — Child Protection & Reformation

Section 210.025 RSMo. — Criminal Background checks, persons receiving state or federal funds for child care, procedures — rulemaking authority.

Section 210.117 RSMo. — **(Until December 31, 2016) Child not reunited with parents or placed in a home, when** ... A child taken into the custody of the state shall not be reunited with the parent or placed in a home in which the parent or any person residing in the home has been found guilty of, or pled guilty to, any of the following offenses when a child was the victim ...

Section 210.117 RSMo. **— (Beginning January 1, 2017) Child not reunited with parents or placed in a home when** ... A child taken into the custody of the state shall not be reunited with the parent or placed in a home in which the parent or any person residing in the home has been found guilty of any of the following offenses when a child was the victim ...

Section 210.160 RSMo. — Guardian ad litem, how appointed — when — fee — volunteer advocates may be appointed to assist — training program.

Section 210.482 RSMo. — If the emergency placement of a child in a private home is necessary due to the unexpected absence of the child's parents, legal guardian, or custodial, the juvenile court or children's division ...

Section 210.487 RSMo. — When conducting investigations of persons for the purpose of foster parent licensing, the division shall ...

Section 210.903 RSMo. — Family care safety registry and access line established, contents.

Chapter 302 — Driver & Commercial Driver Licenses

Section 302.060 RSMo. — License not to be issued to whom, exceptions — reinstatement requirements.

Section 302.309 RSMo. — Return of license, when — limited driving privilege, when granted, application, when denied — judicial review of denial by director of revenue — rulemaking.

Chapter 313 — Licensed Gaming Activities

Section 313.220 RSMo. — Rules and regulations — procedure generally, this chapter — background checks may be required, when.

Section 313.810 RSMo. — Applicants contents, fingerprint submissions — investigations, commission may conduct — false information on application, penalty.

Chapter 453 — Adoption & Foster Care

Section 453.070 RSMo. — Investigation preconditions for adoptions — contents of investigation report — how conducted — assessments of adoptive parents, contents — waving of investigations, when — fees — preference to foster parents, when.

Chapter 571 — Weapons Offenses — Concealed Carry Permits

Section 571.101 RSMo. — Concealed carry endorsement, application requirements, approval procedures, issuance of certificates, when, record keeping requirements, and fees.

Section 571.102 RSMo. — Repealed L. 2013, S.B. 75

Section 571.104 RSMo. — Suspension or revocation of endorsements, when, renewal procedures, change of name of residence notification requirements.

Section 571.107 RSMo. — Endorsement does not authorize concealed firearms, where, penalty for violations.

Section 571.111 RSMo. — Firearms training requirements, safety instructor requirements, penalty for violations.

Section 571.114 RSMo. — Denial of application, appeal procedures.

Section 571.117 RSMo. — Revocation procedures for ineligible certificate holders, sheriff's immunity from liability, when.

Section 571.121 RSMo. — Duty to carry and display permit, penalty for violation, director of revenue immunity from liability, when.

Section 571.126 RSMo. — List of persons who have obtained a concealed carry endorsement or permit, no disclosure to federal government.

Chapter 590 — Police Officers Standards & Training (POST)

Section 590. 060 RSMo. — Minimum standards for training instructors and centers — licensure of instructors — background check required, when.

Chapter 610 — Governmental Bodies and Records

Section 610.120 RSMo. — Records to be confidential — accessible to whom, purposes.

Section 610.122 RSMo. — Arrest record expunge, requirements.

Section 610.123 RSMo. — Procedure to expunge, Missouri Supreme Court to promulgate rules — similar to small claims.

Section 610.126 RSMo. — An expungement of an arrest record shall not reflect on the validity of the arrest and shall not be construed to indicate a lack of probable cause for the arrest.

Section 610.130 RSMo. — Beginning January 1, 2017 — Alcohol-related driving offenses, expunged from records, when— procedures, effect — limitation.

Section 610.140 RSMo. — Expungement of certain criminal records, petition, contents, procedure.

Chapter 621 — Administrative Hearing Commission

Section 621.045 RSMo. — Commission to conduct hearings, make determinations — boards included — settlement agreements – default decision, when. (Referenced in Section 43.543 RSMo.)

****

FEDERAL CRIMINAL HISTORY-RELATED REPORTING LAWS

According to federal law (Title 28 USC 534), the FBI has authority to collect and exchange criminal history record information for criminal justice and noncriminal justice purposes. As complex and diverse as the federal government is, there are several governmental actions that dramatically affect the way a federal agency may use the personal information it houses. Since the FBI has the authority to collect and disseminate criminal history information and criminal history information is considered private, the FBI must abide by federal laws, i.e. the Privacy Act of 1974 and the Freedom of Information Act.

Title 5

Title 5, U.S.C 552, as amended by Public Law 104-231, 110 Stat. 3048, Freedom of Information Act — The U.S. Freedom of Information Act (FOIA) is a law ensuring public access to the U.S. government records. FOIA carries a presumption of disclosure; the burden is on the government, not the public, to substantiate why information may not be released. FOIA allows an individual to consent to the disclosure of information about the individual from federal agencies to third parties. This includes access to an individual's criminal history record maintained by the FBI. There are no restrictions regarding the purpose of a FOIA request and, therefore, an individual could make such a request for his/her FBI criminal record and either provide it to an employer or specify that the record be sent directly to an employer. FBI maintains that the federal Privacy Act of 1974 protects criminal history record information and its disclosure is prohibited without consent from the individual who is the subject of the information or a state statutory exception that authorizes disclosure. (Title 5 USC 552a)

***Title 5 U.S.C. Section 552a,* Privacy Act of 1974** — The Privacy Act reaffirmed an earlier law (Public Law 92-544), in that it specified, "no governmental agency shall disclose any records to any person or agency unless prior written consent is received from the individual or it is used by the agency to perform the duties of the agency." With the Privacy Act of 1974, government agencies may release certain information; however, they must track the dissemination of each record including the time, date, purpose, and to whom the information was disclosed. The information may not be disclosed except for government use or unless it is authorized by applicable law or state statute.

TITLE 42

Title 42 U.S.C. 14616, Part 907 — This rule establishes policies and procedures to ensure that use of the III System for noncriminal justice purposes complies with the National Crime Prevention and Privacy Compact Council (Compact Council) and with rules, standards, and procedures established by the Compact Council regarding application and response procedures, record dissemination and use, response times, data quality, system security, accuracy, privacy protection, and other aspects of III System operation for noncriminal justice purposes. This rule is established pursuant to Article VI of the Compact.

Title 42 U.S.C. 14616, Article V (b) — Each request for a criminal history record check utilizing the national indices made under any approved state statute shall be submitted through the state's criminal history record repository. A state criminal history record repository shall process an interstate request for noncriminal justice purposes through the national indices only if such request is transmitted through another state criminal history record repository or the FBI.

Title 42 U.S.C 14616, Article V (d). Fees. (1) **—** A state criminal history record repository or the FBI may charge a fee, in accordance with applicable law, for handling a request involving fingerprint processing for noncriminal justice purposes.

PUBLIC LAWS

***Public Law 92-544,* Violent Crime Control and Law Enforcement Act** — This act, passed in 1972 by the U.S. congress, is an appropriations statute that provides funding to the FBI for acquiring, collecting, classifying, preserving, and exchanging identification records with duly authorized officials of the federal government, states, cities, and other institutions for the purpose of licensing and employment if authorized by state statute. The law, however, did not provide guidelines for obtaining federal criminal background checks. The authorization to disseminate criminal history information for the purposes of licensing and employment was restricted with a stipulation requiring a state statute authorizing the use of the information and approval by the U.S. attorney general.

Public Law 103-159, The Brady Act, The National Criminal Instant Background Check System (NICS) — Established as part of the Brady Handgun Violence Prevention Act of 1993, it is a national system that

cross-references NCIC, III, and the NICS index to search for individuals that are, by federal law, prohibited from receiving firearms.

Public Law 103-209 — The National Child Protection Act (NCPA) allows access to FBI criminal history for qualified entities providing care to children, the elderly, or individuals with disabilities.

Public Law 104-120, Title 42 — The Housing Opportunity Program Extension Act of 1996, followed by the Quality Housing and Work Responsibility Act of 1998 (Public Law 105-276), allows the administrators and officials of the U.S. Department of Housing and Urban Development (HUD) authority to obtain criminal history records from the FBI for the purpose of applicant screening, lease enforcement, and eviction.

Public Law 105-251, **Volunteers for Children Act (VCA)** — This act amended the NCPA/VCA of 1993, and further expanded the ability to receive criminal history to protect children, the elderly, and individuals with disabilities.

Public Law 108-458, **Section 6402 of the Intelligence Reform and Terrorism Prevention Act of 2004, included the Private Security Officer Employment Authorization Act** — Authorizes a fingerprint-based criminal history check of state and national criminal history records to screen prospective and current private security officers.

Public Law 109-248, **Adam Walsh Child Protection & Safety Act,** ***Sections 151 and 153, Adam Walsh Child Protection and Safety Act of 2006*** — Requires the attorney general to ensure access to FBI criminal history record information by (1) governmental social service agencies with child protection responsibilities, (2) child welfare agencies, and (3) public and private elementary and secondary schools and state and local educational agencies.

Section 151, Public Law 109-248, Adam Walsh Child Protection & Safety Act — This act provides that access by governmental social service agencies with child protection responsibilities is to be used only in investigating or responding to reports of child abuse, neglect, or exploitation. An ORI with an "F" in the ninth position is required and purpose code C must be used when making III queries.

Section 153, Public Law 109-248, Adam Walsh Child Protection & Safety Act, Schools SAFE Act — "Schools Safely Acquiring Faculty Excellence Act of 2006" — This act allows for fingerprint-based checks of national crime information databases (as defined in 28 U.S.C. Section 534) by private or public elementary or secondary schools, or local or state educational agencies.

Public Law 111-13, The Edward M. Kennedy Serve America Act — This act requires volunteers working with vulnerable citizens be background checked through FBI.

TITLE 28

28 United States Code (USC) 534 — This code pertains to acquisition, preservation, and exchange of identification records and information, appointment of officials.

Title 28, Code of Federal Regulations (CFR) Part 901 — This code outlines fingerprint submission requirements. The Compact provides that "subject's fingerprints or other approved forms of positive identification shall be submitted with all requests for criminal history record checks for noncriminal justice purposes." (Title 42 USC 14616 Article V (a). The Compact recognizes the extreme reliability of fingerprint-based identifications and requires that fingerprints be submitted contemporaneously with search requests whenever feasible. (Exception to this rule is exigent circumstances, 28 CFR 901.2(a) (2), which is also approved in Section 210.482 RSMo.)

Title 28, CFR 901.1 — This code applies to the required submission of fingerprints, along with requests for III records, by agencies authorized to access and receive criminal history records under Public Law 92-544. It establishes protocols and procedures applicable to the III and its use for noncriminal justice purposes.

Title 28, CFR 901.2 — (a) Article V of the Compact requires the submission of fingerprints or other approved forms of positive identification with requests for criminal history record checks for noncriminal justice purposes. The requirement for the submission of fingerprints may be satisfied in two ways: (1) The fingerprints should be submitted contemporaneously with the request for criminal history information, or (2) For purposes approved by the Compact, a delayed submission of fingerprints may be permissible under exigent circumstances. (Section 210.482 RSMo.)

Title 28 CFR Part 901.4 — This code states that audits of authorized state agencies that access the III System shall be conducted by the state's Compact Officer ... such audits shall be conducted to verify adherence to the provisions of Part 901 and the FBI's CJIS Security Policy.

Title 28, CFR Part 907 — This code covers Compact Council Procedures for Compliant Conduct and Responsible Use of the III System for Noncriminal Justice Purposes.

Title 28 CFR, Chapter I, Part 20 — This code provides information regarding the National Crime Information Center (NCIC), and preparation and submission of Criminal History Record information to the FBI.

Title 28 CFR 20.33 — This code restricts the use of CHRI. Criminal history records received from the III System or the FIRS shall be used only for the purpose requested and a current record should be requested when needed for a subsequent authorized use.

Title 28 CFR 50.12 — This code addresses the exchange of FBI identification records. Records obtained under this authority may be used solely for the purpose requested and cannot be disseminated outside the receiving departments, related agencies, or other authorized entities.

Note: Federal law sets forth the minimum standards regarding access and use of criminal history record information. The states may make laws more restrictive, but not less restrictive. (FBI CJIS Audit Aug. 2009)

APPENDIX E: WEBSITE LINKS

- Missouri State Highway Patrol website: http://www.mshp.dps.mo.gov
- The Missouri Automated Criminal History Site (MACHS): https://www.machs.mshp.dps.mo.gov/MACHSFP/home.html
- CJIS On-Line Security Awareness Training: http://www.cjisonline.com
- Revised Statutes of Missouri: http://www.moga.mo.gov/mostatutes/statutesAna.html
- FBI Website: http://www.fbi.gov/
- VECHS Program and for downloading of program forms: http://www.mshp.dps.missouri.gov/MSHPWeb/PatrolDivisions/CRID/MoVECHSProgram.html
- Applicant Privacy Rights: http://www.mshp.dps.missouri.gov/MSHPWeb/PatrolDivisions/CRID/ApplicantPrivacyRights.html
- http://www.fbi.gov/about-us/cjis/cc/library/noncriminal-justice-applicants-privacy
- FBI CJIS Security Policy: http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view

APPENDIX F: SAMPLE DOCUMENTS

- Ordinance Wording — City/County Governments
- ORI Letter of Request — City/County Governments
- ORI Letter of Request — Generic Use
- Concealed Carry Permits, Denial of Permit
- Security Incident Report
- Sample Dissemination Log

Suggested Language – Ordinance Wording For City/County Government

[¶ Enter Ordinance Number]

This ordinance is enacted pursuant to Section 43.535 RSMo., to regulate the issuance of licenses for [list occupations, i.e. liquor licenses, solicitors/peddlers, etc.] within the [enter name of city or county] or employment with [enter name of city or county government].

An [applicant, employee, prospective employee, or volunteer] seeking to engage in [list occupation(s)] shall submit his/her fingerprints to the Missouri State Highway Patrol Criminal Justice Information Services (CJIS) Division along with appropriate fees. The Missouri State Highway Patrol CJIS Division will compare the subject's fingerprints against its criminal file and, if necessary, submit the fingerprints to the Federal Bureau of Investigation for a comparison with national criminal history records. The results of the Federal Bureau of Investigation check will be returned to the Missouri State Highway Patrol CJIS Division, which will disseminate the state and national results to [enter name of city or county government].

The [enter name of city/county government] shall render a fitness determination based upon the results of the criminal background check. In rendering a fitness determination, the [enter name of city/county government] will decide whether the subject of record has been convicted of or is under pending indictment for (a) a crime which bears upon his/her ability or fitness to serve in that capacity; (b) any felony or a misdemeanor which involved force or threat of force, controlled substances, or a sex-related offense; or (c) enumerated disqualifiers.

The subject of record may request and receive a copy of his/her criminal history record information from the [enter name of city/county government]. Should the subject of record seek to amend or correct his/her record, he/she must contact the Missouri State Highway Patrol CJIS Division for a Missouri state record and the Federal Bureau of Investigation for records from other state jurisdictions maintained in its file.

ORI Request
For City/County Governments
Pursuant To Section 43.535 RSMo.

Captain Larry W. Plunkett Jr., Director
Criminal Justice Information Services Division
Missouri State Highway Patrol
1510 E. Elm Street
P. O. Box 9500
Jefferson City, MO 65102-9500

Dear Captain Plunkett:

The [enter name of city or county government] would like to formally request an Originating Agency Identifier (ORI) for use in submitting applicant fingerprints for receipt of state and national criminal history record information pursuant to our Ordinance No. [enter Ordinance #].

It is our understanding with the passage of this ordinance we have met the Public Law 92-544 criteria and Section 43.535 RSMo., to conduct background checks on applicants and licensees in specific occupations including [list the occupations that are specified in the ordinance]. A copy of our ordinance is attached for your review.

Upon approval, we ask that the background check results be forwarded to the attention of:

Agency Point of Contact
Agency Name
Address
City, State Zip
Telephone Number

Thank you for your assistance with this request. Should you have any questions or need additional information, please do not hesitate to contact me.

Sincerely,

[Insert Name]

Enclosure: [copy of ordinance]

ORI Request
For Agency Use (Generic)

[Date]

Captain Larry W. Plunkett Jr., Director
Criminal Justice Information Services Division
Missouri State Highway Patrol
P.O. Box 9500
Jefferson City, MO 65102-9500

Dear Captain Plunkett:

The [enter name of agency] requests an Originating Agency Identifier (ORI) for use when fingerprinting applicants through the state and Federal Bureau of Investigation. The reason for the background check is for eligibility determinations for [enter purpose(s)] within the [enter name of agency] as authorized in [enter state statute].

It is our understanding that with the submission of fingerprints and pursuant to the authority in [enter state statute] that state and federal background checks are authorized. Upon approval, we ask that the background check results be forwarded to the attention of:

Agency Point of Contact
Agency Name
Address
City, State Zip
Telephone Number

Thank you for your assistance with this request. Should you have any questions, please do not hesitate to give me a call.

Sincerely,

(Insert name)

SAMPLE DENIAL LETTER
-- CONCEALED CARRY PERMITS --
(Letter can serve as dissemination documentation.)

Date

Applicant Name
Address
City, State Zip

Dear (Applicant):

The purpose of this letter is to inform you that your request for a Concealed Carry Permit has been denied. According to Section 571.101 RSMo., the sheriff may refuse to approve an application if it is determined that any of the requirements specified in Subsection 2 have not been met or there is substantial and demonstrable reason to believe that the applicant has rendered a false statement regarding any of the provisions listed in Sections 571.101 to 571.121 RSMo.

As stated in Section 571.114 RSMo., you have the right to appeal the denial within 30 days of receiving written notice of the denial.

Your application for a Concealed Carry Permit has been denied for the following reason(s):

- [List reason(s) here]

A copy of Section 571.114 RSMo. and a copy of your fingerprint-based criminal history responses are included with this letter. Please feel free to contact my office should you have any questions.

Sincerely,

[Insert Name]

Enclosures

SHP-71 03/15

MISSOURI STATE HIGHWAY PATROL
SECURITY INCIDENT REPORT
(NONCRIMINAL JUSTICE AGENCIES)

PLEASE PRINT OR TYPE

Reset Form | Print Form

Agency Information			
Agency Name		Agency ORI/OCA	
Address	City	State	Zip Code
Area Code and Telephone Number	Fax Number		

Point of Contact	
Last Name	First Name
Email Address	Area Code and Telephone Number

Incident Details	
Date of Incident	Time of Incident Discovery (e.g., 1400)
Location of Incident	
Systems/Data Affected	Method of Detection

Nature of the Incident (Please Check One)

☐ Systems/Data Misuse ☐ Virus/Malware ☐ Network Intrusion ☐ Data Loss/Data Breach ☐ Unauthorized Access
☐ Denial of Service ☐ Unauthorized Changes ☐ Theft/Loss of Device ☐ Other (Explain)

Incident Description

Current Incident Status (Please Check One)

☐ Contained ☐ Uncontained ☐ Investigating ☐ Other (Explained in Incident Description)

System Impact (Please Check One)

☐ Complete Outage ☐ Partial Outage ☐ No Impact ☐ Other (Explained in Incident Description)

CJIS Information Security Unit (ISU) Assistance requested (Please Check One)

☐ Yes ☐ No

Resolution

Return completed form to:

MSHP
CJIS Security Unit
PO Box 9500
Jefferson City, MO 65102-9500
Fax: (573) 526-6290
cjissecurity@mshp.dps.mo.gov
For questions, call (573) 526-6153 ext 2658

CHRI Secondary Dissemination Record	Date of Secondary Dissemination
Information About Original CHRI Request	
Subject's Name (Last, First, MI)	Date of Birth (optional)
Agency Name	Date Requested
Information About Secondary CHRI Dissemination	
Name of Requestor/Agency	Purpose of Request
Address	**Signature of Person Receiving CHRI (if in person)**

NOTE: This form is provided as a sample and may be used "as is" to document any secondary dissemination made by your agency. A copy is to be retained in the agency file until the agency has received a successful Policy Compliance Review from the MSHP.

Violations and associated penalties for misuse of dissemination practices are stated in Section 576.050 RSMo., Section 43.532 RSMo., and Title 18 United States Code.

Bibliography

Criminal Justice Information Services (CJIS) Security Policy, U.S. Department of Justice, Federal Bureau of Investigation CJIS Division, CJISD-ITS-DOC-08140-5.3, 2014.

Missouri Uniform Law Enforcement System (MULES) Policy and Procedures Manual, Missouri State Highway Patrol CJIS Division, 2014.

NCIC Operating Manual, U.S. Department of Justice, Federal Bureau of Investigation, 2015.

Standard Operating Procedures, Missouri State Highway Patrol CJIS Division, 2015.

Questions or comments regarding the information contained within this document may be directed to:

Missouri State Highway Patrol
Criminal Justice Information Services Division – NCJ Audit/Training Unit
1510 E. Elm Street
P. O. Box 9500
Jefferson City, MO 65102-9500
Telephone Number: (573) 526-6153
Fax Number: (573) 751-9382